

Intro Abstract Algebra

©1997-8, Paul Garrett, garrett@math.umn.edu
<http://www.math.umn.edu/~garrett/>

Contents

- (1) Basic Algebra of Polynomials
- (2) Induction and the Well-ordering Principle
- (3) Sets
- (4) Some counting principles
- (5) The Integers
- (6) Unique factorization into primes
- (7) (*) Prime Numbers
- (8) Sun Ze's Theorem
- (9) Good algorithm for exponentiation
- (10) Fermat's Little Theorem
- (11) Euler's Theorem, Primitive Roots, Exponents, Roots
- (12) (*) Public-Key Ciphers
- (13) (*) Pseudoprimes and Primality Tests
- (14) Vectors and matrices
- (15) Motions in two and three dimensions
- (16) Permutations and Symmetric Groups
- (17) Groups: Lagrange's Theorem, Euler's Theorem
- (18) Rings and Fields: definitions and first examples
- (19) Cyclotomic polynomials
- (20) Primitive roots
- (21) Group Homomorphisms
- (22) Cyclic Groups
- (23) (*) Carmichael numbers and witnesses
- (24) More on groups
- (25) Finite fields
- (26) Linear Congruences
- (27) Systems of Linear Congruences
- (28) Abstract Sun Ze Theorem
- (29) (*) The Hamiltonian Quaternions
- (30) More about rings
- (31) Tables

1. Basic Algebra of Polynomials

Completing the square to solve a quadratic equation is perhaps the first really good trick in elementary algebra. It depends upon appreciating the form of the square of the *binomial* $x + y$:

$$(x + y)^2 = x^2 + xy + yx + y^2 = x^2 + 2xy + y^2$$

Thus, running this backwards,

$$\begin{aligned}x^2 + ax &= x^2 + 2\left(\frac{a}{2}\right)x = x^2 + 2\left(\frac{a}{2}\right)x + \left(\frac{a}{2}\right)^2 - \left(\frac{a}{2}\right)^2 \\ &= \left(x + \frac{a}{2}\right)^2 - \left(\frac{a}{2}\right)^2\end{aligned}$$

Then for $a \neq 0$,

$$ax^2 + bx + c = 0$$

can be rewritten as

$$0 = \frac{0}{a} = x^2 + 2\frac{b}{2a}x + \frac{c}{a} = \left(x + \frac{b}{2a}\right)^2 + \frac{c}{a} - \left(\frac{b}{2a}\right)^2$$

Thus,

$$\begin{aligned}\left(x + \frac{b}{2a}\right)^2 &= \left(\frac{b}{2a}\right)^2 - \frac{c}{a} \\ x + \frac{b}{2a} &= \pm \sqrt{\left(\frac{b}{2a}\right)^2 - \frac{c}{a}} \\ x &= -\frac{b}{2a} \pm \sqrt{\left(\frac{b}{2a}\right)^2 - \frac{c}{a}}\end{aligned}$$

from which the usual **Quadratic Formula** is easily obtained.

For positive integers n , we have the **factorial** function defined:

$$n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-2) \cdot (n-1) \cdot n$$

Also, we take $0! = 1$. The fundamental property is that

$$(n+1)! = (n+1) \cdot n!$$

And there is the separate *definition* that $0! = 1$. The latter convention has the virtue that it works out in practice, in the patterns in which factorials are most often used.

The **binomial coefficients** are numbers with a special notation

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

The name comes from the fact that these numbers appear in the **binomial expansion** (expansion of powers of the *binomial* $(x + y)$):

$$\begin{aligned}(x + y)^n &= \\ x^n + \binom{n}{1} x^{n-1}y + \binom{n}{2} x^{n-2}y^2 + \dots + \binom{n}{n-2} x^2y^{n-2} + \binom{n}{n-1} xy^{n-1} + y^n\end{aligned}$$

$$= \sum_{0 \leq i \leq n} \binom{n}{i} x^{n-i} y^i$$

Notice that

$$\binom{n}{n} = \binom{n}{0} = 1$$

There are **standard identities** which are useful in anticipating factorization of special polynomials and special forms of numbers:

$$\begin{aligned} x^2 - y^2 &= (x - y)(x + y) \\ x^3 - y^3 &= (x - y)(x^2 + xy + y^2) & x^3 + y^3 &= (x + y)(x^2 - xy + y^2) \\ x^4 - y^4 &= (x - y)(x^3 + x^2y + xy^2 + y^3) \\ x^5 - y^5 &= (x - y)(x^4 + x^3y + x^2y^2 + xy^3 + y^4) \\ x^5 + y^5 &= (x + y)(x^4 - x^3y + x^2y^2 - xy^3 + y^4) \end{aligned}$$

and so on. Note that for *odd* exponents there are *two* identities while for *even* exponents there is just *one*.

#1.1 Factor $x^6 - y^6$ in two different ways.

#1.2 While we mostly know that $x^2 - y^2$ has a factorization, that $x^3 - y^3$ has a factorization, that $x^3 + y^3$ has, and so on, there is a factorization that seldom appears in 'high school': $x^4 + 4y^4$ has a factorization into two quadratic pieces, each with 3 terms! Find this factorization. *Hint:*

$$x^4 + 4y^4 = (x^4 + 4x^2y^2 + 4y^4) - 4x^2y^2 = (x^2 + 2y^2)^2 - (2xy)^2$$

2. Induction and the Well-ordering Principle

The meaning of the word ‘induction’ within mathematics is very different from the colloquial sense!

First, let $P(n)$ be a statement involving the integer n , which may be true or false. That is, at this point we have a *grammatically* correct sentence, but are making no general claims about whether the sentence is true, true for *one* particular value of n , true for *all* values of n , or anything. It’s just a sentence.

Now we introduce some notation that is entirely compatible with our notion of *function*, even if the present usage is a little surprising. If the sentence $P(n)$ is true of a particular integer n , write

$$P(n) = \text{true}$$

and if the sentence asserts a *false* thing for a particular n , write

$$P(n) = \text{false}$$

That is, we *can* view P as a *function*, but instead of producing *numbers* as output it produces either ‘*true*’ or ‘*false*’ as values. Such functions are called **boolean**.

This style of writing, even if it is not what you already knew or learned, is entirely parallel to ordinary English, is parallel to programming language usage, and has many other virtues.

Caution: There is an *another*, older tradition of notation in mathematics which is somewhat different, which is and which is harder to read and write unless you know the trick, since it is *not* like ordinary English at all. In that *other* tradition, to write ‘ $P(n)$ ’ is to assert that the sentence ‘ $P(n)$ ’ is *true*. In the *other* tradition, to say that the sentence is *false* you write ‘ $\neg P(n)$ ’ or ‘ $\sim P(n)$ ’.

So, yes, these two ways of writing are not compatible with each other. Too bad. We need to make a choice, though, and while I *once* would have chosen what I call the ‘older’ tradition, *now* I like the first way better, for several reasons. In any case, you should be alert to the possibility that other people may choose one or the other of these writing styles, and you have to figure it out from context!

Principle of Induction

- If $P(1) = \text{true}$, and
- if $P(n) = \text{true}$ *implies* $P(n + 1) = \text{true}$ for every positive integer n ,
- then $P(n) = \text{true}$ for *every* positive integer n .

Caution: The second condition does *not* directly assert that $P(n) = \text{true}$, nor does it directly assert that $P(n + 1) = \text{true}$. Rather, it only asserts a *relative* thing. That is, more generally, with some sentences A and B (involving n or not), an assertion of the sort

$$(A \text{ implies } B) = \text{true}$$

does not assert that $A = \text{true}$ nor that $B = \text{true}$, but rather can be re-written as *conditional* assertion

$$\text{if } (A = \text{true}) \text{ then } B = \text{true}$$

In other words we prove that an *implication* is true.

That is, pushing this notation style a little further, we usually prove

$$(A = \text{true}) \text{ implies } B = \text{true} = \text{true}$$

In the more traditional notation, the assertion of Mathematical Induction is

- If $P(1)$, and
- if $P(n)$ implies $P(n + 1)$ for every positive integer n ,
- then $P(n)$ for every positive integer n . Even though I am accustomed to this style of writing, in the end I think it is less clear!

Another Caution: Whatever the notation we use, the statements above do not indicate the way that we usually go about proving something by induction. Rather, what we use is **Practical Paraphrase of ‘Principle of Induction’**:

- First, *prove* $P(1) = \text{true}$.
- Second, *assume* $P(n) = \text{true}$ and using this *prove* $P(n + 1) = \text{true}$ (for every positive integer n)
- Then *conclude* $P(n) = \text{true}$ for every positive integer n .

The second item in this procedure is what is usually called **the induction step**. Our paraphrase makes it look a little different than the more official version: in the official version, it looks like we have to prove that an *implication* is correct, whereas by contrast in our modified version we instead *assume* something true and see if we can then prove something else.

The most popular traditional example is to prove by induction that

$$1 + 2 + 3 + 4 + \dots + (n - 2) + (n - 1) + n = \frac{1}{2}n(n + 1)$$

Let $P(n) = \text{true}$ be the assertion that this formula holds for a particular integer n . So the assertion $P(1) = \text{true}$ is just the assertion that

$$1 = \frac{1}{2}1(1 + 1)$$

which is indeed true. To do the induction step, we *assume* that

$$1 + 2 + 3 + 4 + \dots + (n - 2) + (n - 1) + n = \frac{1}{2}n(n + 1)$$

is true and try to prove from it that

$$1 + 2 + 3 + 4 + \dots + (n - 2) + (n - 1) + n + (n + 1) = \frac{1}{2}(n + 1)((n + 1) + 1)$$

is true.

Well, if we add $n + 1$ to both sides of the *assumed* equality

$$1 + 2 + 3 + 4 + \dots + (n - 2) + (n - 1) + n = \frac{1}{2}n(n + 1)$$

then we have

$$1 + 2 + 3 + 4 + \dots + (n - 2) + (n - 1) + n + (n + 1) = \frac{1}{2}n(n + 1) + (n + 1)$$

The left-hand side is just what we want, but the right hand side is not. But we *hope* that it secretly *is* what we want; that is, we *hope* that

$$\frac{1}{2}n(n+1) + (n+1) = \frac{1}{2}(n+1)((n+1)+1)$$

We have to check that this is true.

This raises an auxiliary question, which is easy enough to answer once we make it explicit: *how would a person go about proving that two polynomials are equal?* The answer is that both of them should be simplified and rearranged in descending (or ascending) powers of the variable, and then check that *corresponding coefficients are equal*. (And this description definitely presumes that we have polynomials in just one variable.)

In the present example it's not very hard to do this rearranging: first, one side of the desired equality simplifies and rearranges to

$$\frac{1}{2}n(n+1) + (n+1) = \frac{1}{2}n^2 + \frac{1}{2}n + n + 1 = \frac{1}{2}n^2 + \frac{3}{2}n + 1$$

On the other hand, the other side of the desired equality simplifies and rearranges to

Or we can try to be a little lucky and just directly rearrange one side of the desired equality of polynomials into the other: in simple situations this works, and if you have some luck, but is *not* the general approach. Still, we can manage it in this example:

$$\begin{aligned} \frac{1}{2}n(n+1) + (n+1) &= \left(\frac{1}{2}n+1\right)(n+1) = \frac{1}{2}(n+2)(n+1) = \\ &= \frac{1}{2}(n+1)(n+2) = \frac{1}{2}(n+1)((n+1)+1) \end{aligned}$$

Thus, we can conclude that *if*

$$1 + 2 + 3 + 4 + \dots + (n-2) + (n-1) + n = \frac{1}{2}n(n+1)$$

then

$$1 + 2 + 3 + 4 + \dots + (n-2) + (n-1) + n + (n+1) = \frac{1}{2}(n+1)((n+1)+1)$$

which is the *implication* we must prove to complete the induction step. Thus, we conclude that this formula really does hold for all positive integers n .

In this example, we used the fact that we knew what we were supposed to be getting to help us do the elementary algebra to complete the induction step. We certainly needed to know what the right formula was before attempting to prove it! This is typical of this sort of argument!

In some circumstances, a seemingly different proof concept works better:

Well-Ordering Principle Every *non-empty* subset of the positive integers has a least element.

This Well-Ordering Principle sounds completely innocuous, but it is provably *logically equivalent* to the Principle of Induction. Another logically equivalent variant is:

Let P be a property that an integer may or may not have. If $P(1) = \text{true}$, and if $P(m) = \text{true}$ for all $m < n$ *implies* that $P(n) = \text{true}$, then P holds for *all* integers.

In the other notation, this would be written

Let P be a property that an integer may or may not have. If $P(1)$, and if $P(m)$ for all $m < n$ implies that $P(n)$, then P holds for *all* integers.

#2.3 Prove by induction that

$$1 + 2 + 3 + \dots + n = \frac{1}{2}n(n+1)$$

#2.4 Prove by *induction* on n that

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + x^{n-3} + \dots + x^2 + x + 1)$$

Hint: To do the induction step, notice that

$$x^{n+1} - 1 = x^{n+1} - x + x - 1 = x(x^n - 1) + (x - 1)$$

#2.5 Prove by induction that

$$1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$$

#2.6 Prove by induction the following relation among binomial coefficients:

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

for integers $0 < k \leq n$.

#2.7 (*) Prove by induction that

$$(1 + 2 + 3 + \dots + n)^2 = 1^3 + 2^3 + 3^3 + \dots + n^3$$

#2.8 (***) How would one systematically obtain the “formula” for $1^k + 2^k + 3^k + \dots + (n-1)^k + n^k$ for a fixed positive integer exponent k ?

3. Sets

- Sets and functions
 - Equivalence relations
-

3.1 Sets

Here we review some relatively elementary but very important terminology and concepts about *sets* and *functions*, in a slightly abstract setting. We use the word **map** as a synonym for “function”, as is very often done.

Naively, a **set** is supposed to be a collection of ‘things’ (?) described by ‘listing’ them or prescribing them by a ‘rule’. Please note that this is *not* a terribly precise description, but will be adequate for most of our purposes. We can also say that a **set** is an *unordered list of different* things.

There are standard symbols for some often-used sets:

$$\phi = \{\} = \text{set with no elements}$$

$$\mathbf{Z} = \text{the integers}$$

$$\mathbf{Q} = \text{the rational numbers}$$

$$\mathbf{R} = \text{the real numbers}$$

$$\mathbf{C} = \text{the complex numbers}$$

A set described by a *list* is something like

$$S = \{1, 2, 3, 4, 5, 6, 7, 8\}$$

which is the set of integers bigger than 0 and less than 9. This set can also be described by a *rule* by

$$S = \{1, 2, 3, 4, 5, 6, 7, 8\} = \{x : x \text{ is an integer and } 1 \leq x \leq 8\}$$

This follows the general format and notation

$$\{x : x \text{ has some property}\}$$

If x is in a set S , then write $x \in S$ or $S \ni x$, and say that x is an *element* of S . Thus, a set is the collection of all its elements (although this remark only explains the *language*). It is worth noting that the *ordering* of a listing has no effect on a set, and if in the listing of elements of a set an element is *repeated*, this has no effect. For example,

$$\{1, 2, 3\} = \{1, 1, 2, 3\} = \{3, 2, 1\} = \{1, 3, 2, 1\}$$

A **subset** T of a set S is a set all of whose elements are elements of S . This is written $T \subset S$ or $S \supset T$. So always $S \subset S$ and $\emptyset \subset S$. If $T \subset S$ and $T \neq \emptyset$ and $T \neq S$, then T is a **proper** subset of S . Note that the empty set is a subset of *every* set. For a subset T of a set S , the **complement** of T (inside S) is

$$T^c = S - T = \{s \in S : s \notin T\}$$

Sets can also be elements of other sets. For example, $\{\mathbf{Q}, \mathbf{Z}, \mathbf{R}, \mathbf{C}\}$ is the set with 4 elements, each of which is a familiar set of numbers. Or, one can check that

$$\{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$$

is the set of two-element subsets of $\{1, 2, 3\}$.

The **intersection** of two sets A, B is the collection of all elements which lie in *both* sets, and is denoted $A \cap B$. Two sets are **disjoint** if their intersection is \emptyset . If the intersection is *not* empty, then we may say that the two sets **meet**. The **union** of two sets A, B is the collection of all elements which lie in *one or the other* of the two sets, and is denoted $A \cup B$.

Note that, for example, $1 \neq \{1\}$, and $\{\{1\}\} \neq \{1\}$. That is, the *set* $\{a\}$ with sole element a is *not* the same thing as the item a itself.

An **ordered pair** (x, y) is just that, a list of two things in which there is a *first* thing, here x , and a *second* thing, here y . Two ordered pairs (x, y) and (x', y') are **equal** if and only if $x = x'$ and $y = y'$.

The **(cartesian) product** of two sets A, B is the set of **ordered pairs** (a, b) where $a \in A$ and $b \in B$. It is denoted $A \times B$. Thus, while $\{a, b\} = \{b, a\}$ might be thought of as an *unordered* pair, for *ordered* pairs $(a, b) \neq (b, a)$ unless by chance $a = b$.

In case $A = B$, the cartesian power $A \times B$ is often denoted A^2 . More generally, for a fixed positive integer n , the n^{th} **cartesian power** A^n of a set is the set of ordered n -tuples (a_1, a_2, \dots, a_n) of elements a_i of A .

Some very important examples of cartesian powers are those of \mathbf{R} or \mathbf{Q} or \mathbf{C} , which arise in other contexts as well: for example, \mathbf{R}^2 is the collection of ordered pairs of real numbers, which we use to describe points in the plane. And \mathbf{R}^3 is the collection of ordered triples of real numbers, which we use to describe points in three-space.

The **power set** of a set S is the *set of subsets* of S . This is sometimes denoted by $\mathcal{P}S$. Thus,

$$\mathcal{P}\emptyset = \{\emptyset\}$$

$$\mathcal{P}\{1, 2\} = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$

Intuitively, a **function** f from one set A to another set B is supposed to be a ‘rule’ which assigns to each element $a \in A$ an element $b = f(a) \in B$. This is written as

$$f : A \rightarrow B$$

although the latter notation gives no information about the nature of f in any detail.

More rigorously, but less intuitively, we can define a ‘function’ by really telling its *graph*: the formal definition is that a function $f : A \rightarrow B$ is a *subset* of the product $A \times B$ with the property that for every $a \in A$ there is a unique $b \in B$ so that $(a, b) \in f$. Then we would write $f(a) = b$.

This formal definition is worth noting at least because it should make clear that there is absolutely no requirement that a function be described by any recognizable or simple ‘formula’.

As a silly example of the formal definition of function, let $f : \{1, 2\} \rightarrow \{2, 4\}$ be the function ‘multiply-by-two’, so that $f(1) = 2$ and $f(2) = 4$. Then the ‘official’ definition would say that really f is the subset of the product set $\{1, 2\} \times \{2, 4\}$ consisting of the ordered pairs $(1, 2), (2, 4)$. That is, formally the function f is the *set*

$$f = \{(1, 2), (2, 4)\}$$

Of course, no one often really operates this way.

A function $f : A \rightarrow B$ is **surjective** (or **onto**) if for every $b \in B$ there is $a \in A$ so that $f(a) = b$. A function $f : A \rightarrow B$ is **injective** (or **one-to-one**) if $f(a) = f(a')$ implies $a = a'$. That is, f is *injective* if for every $b \in B$ there is *at most one* $a \in A$ so that $f(a) = b$. A map is a **bijection** if it is both injective and surjective.

The number of elements in a set is its **cardinality**. Two sets are said to **have the same cardinality** if there is a *bijection* between them. Thus, this is a trick so that we don’t have to actually *count* two sets to see whether they have the same number of elements. Rather, we can just pair them up by a *bijection* to achieve this purpose.

Since we *can* count the elements in a *finite* set in a traditional way, it is clear that *a finite set has no bijection to a proper subset of itself*. After all, a proper subset has *fewer elements*.

By contrast, for *infinite* sets it is easily possible that *proper* subsets have bijections to the whole set. For example, the set A of *all* natural numbers and the set E of *even* natural numbers have a bijection between them given by

$$n \rightarrow 2n$$

But certainly E is a *proper* subset of A ! Even more striking examples can be arranged. In the end, we take as *definition* that a set is **infinite** if it has a bijection to a proper subset of itself.

Let $f : A \rightarrow B$ be a function from a set A to a set B , and let $g : B \rightarrow C$ be a function from the set B to a set C . The **composite function** $g \circ f$ is defined to be

$$(g \circ f)(a) = g(f(a))$$

for $a \in A$.

The **identity function** on a non-empty set S is the function $f : S \rightarrow S$ so that $f(a) = a$ for all $a \in A$. Often the identity function on a set S is denoted by id_S .

Let $f : A \rightarrow B$ be a function from a set A to a set B . An **inverse function** $g : B \rightarrow A$ for f (if such g exists at all) is a function so that $(f \circ g)(b) = b$ for all $b \in B$, and also $(g \circ f)(a) = a$ for all $a \in A$. That is, the inverse function (if it exists) has the two properties

$$f \circ g = \text{id}_B \quad g \circ f = \text{id}_A$$

An inverse function to f , if it exists at all, is usually denoted f^{-1} . (This is *not* at all the same as $1/f$!)

Proposition: A function $f : A \rightarrow B$ from a set A to a set B has an inverse if and only if f is a bijection. In that case, the inverse is unique (that is, there is only *one* inverse function).

Proof: We define a function $g : B \rightarrow A$ as follows. Given $b \in B$, let $a \in A$ be an element so that $f(a) = b$. Then define $g(b) = a$. Do this for each $b \in B$ to define g . Note that we use the *surjectivity* to know that there *exists* an a for each b , and the *injectivity* to be sure of its *uniqueness*.

To check that $g \circ f = \text{id}_A$, compute: first, for any $a \in A$, $f(a) \in B$. Then $g(f(a))$ is, by definition, an element $a' \in A$ so that $f(a') = f(a)$. Since f is injective, it must be that $a' = a$. To check that $f \circ g = \mathbf{1}$, take $b \in B$ and compute: by definition of g , $g(b)$ is an element of A so that $f(g(b)) = b$. But that is (after all) just what we want. *Done*.

3.2 Equivalence Relations

The idea of **equivalence relation** (defined below) is an important extension and generalization of the traditional idea of *equality*, and occurs throughout mathematics. The associated idea of **equivalence class** (also defined just below) is equally important.

The goal here is to make precise both the idea and the notation in writing something like “ $x \sim y$ ” to mean that x and y have some specified common feature. We can set up a general framework for this without worrying about the specifics of what the features might be.

Recall the “formal” definition of a *function* f from a set S to a set T : while we *think of* f as being some sort of rule which to an input $s \in S$ “computes” or “associates” an output $f(s) \in T$, this way of talking is inadequate, for many reasons.

Rather, the formal (possibly non-intuitive) definition of function f from a set S to a set T is that it is a subset G of the cartesian product $S \times T$ with the property

- For each $s \in S$ there is exactly one $t \in T$ so that $(s, t) \in G$.

Then connect this to the usual notation by

$$f(s) = t \quad \text{if} \quad (s, t) \in G$$

(Again, this G would be the *graph* of f if S and T were simply the real line, for example).

In this somewhat formal context, first there is the primitive general notion of **relation** R on a set S : a *relation* R on a set S is simply a subset of $S \times S$. Write

$$x R y$$

if the ordered pair (x, y) lies in the subset R of $S \times S$.

This definition of “relation” compared to the formal definition of “function” makes it clear that every function is a relation. But most relations do not meet the condition to be functions. This definition of “relation” is not very interesting except as set-up for further development.

An **equivalence relation** R on a set S is a special kind of relation, satisfying

- **Reflexivity**: $x R x$ for all $x \in S$
- **Symmetry**: If $x R y$ then $y R x$
- **Transitivity**: If $x R y$ and $y R z$ then $x R z$

The fundamental example of an equivalence relation is ordinary equality of numbers. Or equality of sets. Or any other version of ‘equality’ to which we are accustomed. It should also be noted that a very popular notation for an equivalence relation is

$$x \sim y$$

(that is, with a tilde rather than an ‘R’). Sometimes this is simply read as x *tilde* y , but also sometimes as x **is equivalent to** y with only *implicit* reference to the equivalence relation.

A simple example of an equivalence relation on the set \mathbf{R}^2 can be defined by

$$(x, y) \sim (x', y') \quad \text{if and only if} \quad x = x'$$

That is, in terms of analytic geometry, two points are *equivalent* if and only if they lie on the same vertical line. Verification of the three required properties in this case is easy, and should be carried out by the reader.

Let \sim be an equivalence relation on a set S . For $x \in S$, the \sim - **equivalence class** \bar{x} containing x is the subset

$$\bar{x} = \{x' \in S : x' \sim x\}$$

The **set of equivalence classes** of \sim on S is denoted by

$$S / \sim$$

(as if we were taking a quotient of some sort). Every element $z \in S$ is certainly contained in an equivalence class, namely the equivalence class of all $s \in S$ so that $s \sim z$.

Note that in general an equality $\bar{x} = \bar{y}$ of equivalence classes \bar{x}, \bar{y} is no indication whatsoever that $x = y$. While it *is* always true that $x = y$ implies $\bar{x} = \bar{y}$, in general there are many *other* elements in \bar{x} than just x itself.

Proposition: Let \sim be an equivalence relation on a set S . If two equivalence classes \bar{x}, \bar{y} have any common element z , then $\bar{x} = \bar{y}$.

Proof: If $z \in \bar{x} \cap \bar{y}$, then $z \sim x$ and $z \sim y$. Then for any $x' \in \bar{x}$, we have

$$x' \sim x \sim z \sim y$$

so $x' \sim y$ by transitivity of \sim . Thus, every element $x' \in \bar{x}$ actually lies in \bar{y} . That is, $\bar{x} \subset \bar{y}$. A symmetrical argument, reversing the roles of x and y , shows that $\bar{y} \subset \bar{x}$. Therefore, $\bar{x} = \bar{y}$. *Done.*

It is important to realize that while we tend to refer to an equivalence class in the notational style \bar{x} for some x in the class, there is no requirement to do so. Thus, it is legitimate to say “an equivalence class A for the equivalence relation \sim on the set S ”.

But of course, given an equivalence class A inside S , it may be convenient to *find* x in the set S so that $\bar{x} = A$. Such an x is a **representative** for the equivalence class. Any element of the subset A is a representative, so in general we certainly should *not* imagine that there is a *unique* representative for an equivalence class.

Proposition: Let \sim be an equivalence relation on a set S . Then the equivalence classes of \sim on S are mutually disjoint sets, and their union is all of S .

Proof: The fact that the union of the equivalence classes is the whole thing is not so amazing: given $x \in S$, x certainly lies inside the equivalence class

$$\{y \in S : y \sim x\}$$

Now let A and B be two equivalence classes. Suppose that $A \cap B \neq \phi$, and show that then $A = B$ (as sets). Since the intersection is non-empty, there is some element $y \in A \cap B$. Then, by the definition of “equivalence class”, for all $a \in A$ we have $a \sim y$, and likewise for all $b \in B$ we have $b \sim y$. By transitivity, $a \sim b$. This is true for all $a \in A$ and $b \in B$, so (since A and B are equivalence classes) we have $A = B$. *Done.*

A set \mathcal{S} of non-empty subsets of a set S whose union is the whole set S , and which are mutually disjoint, is called a **partition** of S . The previous proposition can be run the other direction, as well:

Proposition: Let S be a set, and let \mathcal{S} be a set of subsets of S , so that \mathcal{S} is a partition of S . Define a *relation* \sim on S by $x \sim y$ if and only if there is $X \in \mathcal{S}$ so that $x \in X$ and $y \in X$. That is, $x \sim y$ if and only if they both lie in the same element of \mathcal{S} . Then \sim is an *equivalence relation*, and its equivalence classes are the elements of \mathcal{S} .

Proof: Since the union of the sets in \mathcal{S} is the whole set S , each element $x \in S$ is contained in *some* $X \in \mathcal{S}$. Thus, we have the reflexivity property $x \sim x$. If $x \sim y$ then there is $X \in \mathcal{S}$ containing both x and y , and certainly $y \sim x$, so we have symmetry.

Finally, the mutual disjointness of the sets in \mathcal{S} assures that each $y \in S$ lies in just one of the sets from \mathcal{S} . For $y \in S$, let X be the *unique* set from \mathcal{S} which contains y . If $x \sim y$ and $y \sim z$, then it must be that $x \in X$ and $z \in X$, since y lies in no other subset from \mathcal{S} . Then x and z both lie in X , so $x \sim z$, and we have transitivity.

Verification that the equivalence classes are the elements of S is left as an exercise. *Done.*

#3.9 How many elements in the set $\{1, 2, 2, 3, 3, 4, 5\}$? How many in the set $\{1, 2, \{2\}, 3, \{3\}, 4, 5\}$? In $\{1, 2, \{2, 3\}, 3, 4, 5\}$?

#3.10 Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{3, 4, 5, 6, 7\}$. List (without repetition) the elements of the sets $A \cup B$, $A \cap B$, and of $\{x \in A : x \notin B\}$.

#3.11 List all the elements of the *power set* (set of subsets) of $\{1, 2, 3\}$.

#3.12 Let $A = \{1, 2, 3\}$ and $B = \{2, 3\}$. List (without repetition) all the elements of the *cartesian product* set $A \times B$.

#3.13 How many functions are there from the set $\{1, 2, 3\}$ to the set $\{2, 3, 4, 5\}$?

#3.14 How many injective functions are there from $\{1, 2, 3\}$ to $\{1, 2, 3, 4\}$?

#3.15 How many surjective functions are there from $\{1, 2, 3, 4\}$ to $\{1, 2, 3\}$?

#3.16 Show that if $f : A \rightarrow B$ and $g : B \rightarrow C$ are functions with inverses, then $g \circ f$ has an inverse, and this inverse is $f^{-1} \circ g^{-1}$.

#3.17 Show that for a surjective function $f : A \rightarrow B$ there is a **right inverse** g , meaning a function $g : B \rightarrow A$ so that $f \circ g = \text{id}_B$ (but not necessarily $g \circ f = \text{id}_A$.)

#3.18 Show that for an injective function $f : A \rightarrow B$ there is a **left inverse** g , meaning a function $g : B \rightarrow A$ so that $g \circ f = \text{id}_A$ (but not necessarily $f \circ g = \text{id}_B$.)

#3.19 Give a *bijection* from the collection $2\mathbf{Z}$ of *even* integers to the collection \mathbf{Z} of *all* integers.

#3.20 (*) Give a *bijection* from the collection of *all* integers to the collection of *non-negative* integers.

#3.21 (**) Give a *bijection* from the collection of all positive integers to the collection of all rational numbers.

#3.22 (**) This illustrates a hazard in a too naive notion of “rule” for forming a set. Let S be the set of all sets which are not an element of themselves. That is, let

$$S = \{ \text{sets } x : x \notin x \}$$

Is $S \in S$ or is $S \notin S$? (*Hint:* Assuming either that S is or isn't an element of itself leads to a contradiction. What's going on?)

4. Some counting principles

Here we go through some important but still relatively elementary examples of *counting*.

First example: Suppose we have n distinct things, for example the integers from 1 to n inclusive. The question is *how many different orderings or ordered listings*

$$i_1, i_2, i_3, \dots, i_{n-1}, i_n$$

of these numbers are there? (Note that this is in contrast to the *unordered* listing in a *set*). The answer is obtained by noting that there are n choices for the first thing i_1 , then $n - 1$ remaining choices for the second thing i_2 (since we can't reuse whatever i_1 was!), $n - 2$ remaining choices for i_3 (since we can't reuse i_1 nor i_2 , whatever they were!), and so on down to 2 remaining choices for i_{n-1} and then just one choice for i_n . Thus, there are

$$n \cdot (n - 1) \cdot (n - 2) \cdot \dots \cdot 2 \cdot 1 = n!$$

possible orderings of n distinct things.

Second example: How many subsets of k elements are there in a set of n things? There are n possibilities for the first choice, $n - 1$ remaining choices for the second (since the first item is removed), $n - 2$ for the third (since the first and second items are no longer available), and so on down to $n - (k - 1)$ choices for the k th. This number is $n!/(n - k)!$, but is *not* what we want, since it includes a count of all different *orders* of choices. That is,

$$\frac{n!}{(n - k)!} = k! \times \text{the actual number}$$

since we saw in the previous example that there are $k!$ possible orderings of k distinct things. Thus, there are

$$\frac{n!}{k!(n - k)!} = \binom{n}{k}$$

choices of subsets of k elements in a set with n elements. This appearance of a binomial coefficient is *typical*.

Third example: How many *disjoint pairs* of subsets of k elements each are there in a set with n elements, where $2k \leq n$? We just saw that there are $\binom{n}{k}$ choices for the *first* subset with k elements. Then the remaining part of the original set has just $n - k$ elements, so there are $\binom{n - k}{k}$ choices for the *second* subset of k elements. But our counting so far accidentally takes into account a *first* subset and a *second* one, which is not what the question is. By now we know that there are $2! = 2$ choices of ordering of two things (subsets, for example). Therefore, there are

$$\begin{aligned} \frac{1}{2} \binom{n}{k} \binom{n - k}{k} &= \frac{1}{2} \frac{n!}{(n - k)!k!} \frac{(n - k)!}{k!(n - 2k)!} \\ &= \frac{n!}{2 k! k!(n - 2k)!} \end{aligned}$$

pairs of disjoint subsets of k elements each inside a set with n elements.

Generalizing the previous: For integers n, ℓ, k with $n \geq k\ell$, we could ask *how many families of ℓ disjoint subsets of k elements each are there inside a set of n elements?* There are

$$\binom{n}{k}$$

choices for the first subset,

$$\binom{n-k}{k}$$

for the second,

$$\binom{n-2k}{k}$$

for the third, up to

$$\binom{n-(\ell-1)k}{k}$$

for the ℓ th subset. But since *ordering* of these subsets is accidentally counted here, we have to divide by $\ell!$ to have the actual number of families. There is some cancellation among the factorials, so that the actual number is

$$\frac{n!}{\ell! (k!)^{\ell} (n-\ell k)!}$$

#4.23 How many different ways are there to *reorder* the set $\{1, 2, 3, 4\}$?

#4.24 How many choices of 3 things from the list $1, 2, 3, \dots, 9, 10$ (*without* replacement)?

#4.25 How many subsets of $\{1, 2, 3, 4, 5, 6, 7\}$ with exactly 4 elements?

#4.26 How many different choices are there of an *unordered* pair of *distinct* numbers from the set $\{1, 2, \dots, 9, 10\}$? How many choices of *ordered* pair?

#4.27 How many different choices are there of an *ordered* triple of numbers from the set $\{1, 2, \dots, 9, 10\}$?

#4.28 How many subsets of all sizes are there of a set S with n elements? (*Hint*: Go down the list of all elements in the set: for each one you have 2 choices, to *include* it or to *exclude* it. Altogether how many choices?)

#4.29 How many pairs of disjoint subsets A, B each with 3 elements inside the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$?

5. The Integers

- Divisibility
 - The division/reduction algorithm
 - Euclidean algorithm
 - Unique factorization
 - Multiplicative inverses modulo m
 - Integers modulo m
-

5.1 The integers

For two integers d, n , the integer d **divides** n (or is a **divisor** of n) if n/d is an integer. This is equivalent to there being another integer k so that $n = kd$. As equivalent terminology, we may also (equivalently) say that n is a **multiple** of d if d divides n .

A divisor d of n is **proper** if it is not $\pm n$ nor ± 1 . A multiple N of n is **proper** if it is neither $\pm n$. The notation

$$d|n$$

is read as ‘ d divides n ’. Notice that *any* integer d divides 0, since $d \cdot 0 = 0$. On the other hand, the *only* integer 0 divides is itself.

A positive integer is **prime** if it has no proper divisors. That is, it has no divisors but itself, its negative, and ± 1 . Usually we only pay attention to *positive* primes.

The following is the simplest but far from most efficient test for primality. It does have the virtue that if a number is not prime then this process finds the smallest divisor $d > 1$ of the number.

Proposition: A positive integer n is prime if and only if it is not divisible by any of the integers d with $1 < d \leq \sqrt{n}$.

Proof: First, if $d|n$ and $2 < d \leq \sqrt{n}$, then the integer n/d satisfies

$$\sqrt{n} \leq \frac{n}{d} \leq \frac{n}{2}$$

(where we are looking at inequalities among *real* numbers!). Therefore, neither of the two factors d nor n/d is ± 1 nor $\pm n$. So n is not prime.

On the other hand, suppose that n has a proper factorization $n = d \cdot e$, where e is the larger of the two factors. Then

$$d = \frac{n}{e} < \frac{n}{d}$$

gives $d^2 \leq n$, so $d \leq \sqrt{n}$. *Done.*

Two integers are **relatively prime** or **coprime** if for every integer d if $d|m$ and $d|n$ then $d = \pm 1$. Also we may say that m is **prime to** n if they are relatively prime. For a positive integer n , the number of positive

integers less than n and relatively prime to n is denoted by $\varphi(n)$. This is called the **Euler phi function**. (The trial-and-error approach to computing $\varphi(n)$ is suboptimal. We'll get a better method shortly.)

Proposition:

- If $a|b$ and $b|c$ then $a|c$.
- If $d|x$ and $d|y$, then for any integers a, b we have $d|(ax + by)$.

Proof: If $a|b$ then there is an integer k so that $ak = b$. If $b|c$ then there is an integer ℓ so that $b\ell = c$. Then, replacing b by ak in the latter equation, we have

$$c = b\ell = (ak) \cdot \ell = a \cdot (k\ell)$$

so $a|c$.

If $d|x$ then there is an integer m so that $dm = x$. If $d|y$ then there is an integer n so that $dn = y$. Then

$$ax + by = a(md) + b(nd) = (am + bn) \cdot d$$

Thus, $ax + by$ is a multiple of d . *Done.*

5.2 The division/reduction algorithm

For a non-zero integer m , there is the process of **reduction modulo m** , which can be applied to arbitrary integers N . At least if m and N are *positive*, this is exactly the division-with-remainder process of elementary arithmetic, with the quotient discarded: the **reduction modulo m of N** is the remainder when N is divided by n . This procedure is also called the **Division Algorithm**, for that reason.

More precisely, the reduction modulo m of N is the unique integer r so that N can be written as

$$N = q \cdot m + r$$

with an integer q and with

$$0 \leq r < |m|$$

(Very often the word 'modulo' is abbreviated as 'mod'.) The non-negative integer m is the **modulus**. We will use the notation

$$r \% m = \text{reduction of } r \text{ modulo } m$$

For example,

$$10 \% 7 = 3$$

$$10 \% 5 = 0$$

$$12 \% 2 = 0$$

$$15 \% 7 = 1$$

$$100 \% 7 = 2$$

$$1000 \% 2 = 0$$

$$1001 \% 2 = 1$$

In some sources, and sometimes for brevity, this terminology is abused by replacing the phrase 'N reduced mod m' by 'N mod m'. This is not so terrible, but there is also a related but significantly different

meaning that ‘ $N \bmod m$ ’ has, as we will see later. Usually the context will make clear what the phrase ‘ $N \bmod m$ ’ means, but watch out. We will use a notation which is fairly compatible with many computer languages: write

$$x \% m$$

for

$$x \text{ reduced modulo } m$$

Reductions mod m can be computed by hand by the familiar *long division* algorithm. For m and N both *positive*, even a simple hand calculator can be used to easily compute reductions. For example: divide N by m , obtaining a decimal. Remove (by subtracting) the integer part of the decimal, and multiply back by n to obtain the reduction mod m of N .

The process of reduction mod m can also be applied to negative integers. For example,

$$-10 \% 7 = 4 \text{ since } -10 = (-2) \cdot 7 + 4$$

$$-10 \% 5 = 0 \text{ since } -10 = (-2) \cdot 5 + 0$$

$$-15 \% 7 = 6 \text{ since } -15 = (-3) \cdot 7 + 6$$

But neither the hand algorithm nor the calculator algorithm mentioned above give the correct output directly: for one thing, it is not true that the reduction mod m of $-N$ is the negative of the reduction mod m of N . And all our reductions mod m are supposed to be non-negative, besides. For example,

$$10 = 1 \cdot 7 + 3$$

shows that the reduction of $10 \bmod 7$ is 3, but if we simply negate both sides of this equation we get

$$-10 = (-1) \cdot 7 + (-3)$$

That ‘-3’ does not fit our requirements. The trick is to add another multiple of 7 to that ‘-3’, while subtracting it from the $(-1) \cdot 7$, getting

$$-10 = (-1 - 1) \cdot 7 + (-3 + 7)$$

or finally

$$-10 = (-2) \cdot 7 + 4$$

And there is one last ‘gotcha’: in case the remainder is 0, as in

$$14 = 2 \cdot 7 + 0$$

when we negate to get

$$-14 = (-2) \cdot 7 + 0$$

nothing further needs to be done, since that 0 is already in the right range. (If we *did* add another 7 to it, we’d be in the wrong range). Thus, in summary, let r be the reduction of $N \bmod m$. Then the reduction of $-N \bmod m$ is $m - r$ if $r \neq 0$, and is 0 if $r = 0$.

The modulus can be negative, as well: however, it happens that always the reduction of N modulo m is just the reduction of $N \bmod |m|$, so this introduces nothing new.

Note that by our definition the reduction mod m of any integer is always non-negative. This is at variance with several computer languages, where the reduction of a negative integer $-N$ is the negative of the reduction of N . This difference has to be remembered when writing code.

Last, let’s prove *existence* and *uniqueness* of the quotient and remainder in the assertion of the Reduction/Division Algorithm:

Proposition: Given a non-zero integer m and arbitrary integer n , there are unique integers q and r so that $0 \leq r < |m|$ and

$$n = q \cdot m + r$$

Proof: For simplicity, we'll do the proof just for $m > 0$. The case that $m < 0$ is very similar. For fixed n and m , let X be the collection of all integers of the form $n - x \cdot m$. Since x can be positive or negative, and since m is not 0, X contains both positive and negative integers. Let r be the least positive integer in X , and let q be the corresponding ' x ', so that $n - qm = r$.

First, we claim that $0 \leq r < |m|$. If $r \geq |m|$, then $r - m \geq 0$. Since $r - m$ is writeable as $n - (q + 1)m$, it is in the collection X . But $r - m < r$, contradicting the fact that r is the smallest positive integer in X . Thus, it could not have been that $r \geq |m|$, and we conclude that $r < |m|$, as desired.

Next, we prove uniqueness of the q and r . Suppose that

$$qm + r = q'm + r'$$

with $0 \leq r < |m|$ and $0 \leq r' < |m|$. By symmetry, we can suppose that $r \leq r'$ (if not, reverse the roles of r and r' in the discussion). Then

$$(q' - q) \cdot m = r' - r$$

and $r' - r \geq 0$. If $r' - r \neq 0$ then necessarily $q' - q \neq 0$, but if so then

$$r' - r = |r' - r| = |q' - q| \cdot |m| \geq 1 \cdot |m|$$

(Again, $r' - r = |r' - r|$ since $r' - r \geq 0$). But

$$r' - r \leq r' < |m|$$

Putting these together, we get the impossible

$$|m| \leq r' - r < |m|$$

This contradicts the supposition that $r \neq r'$. Therefore, $r = r'$. Then, from $(q' - q)m = r' - r = 0$ (and $m \neq 0$) we get $q' = q$, as well. This proves the uniqueness. *Done.*

Remark: The assertion that any (non-empty) collection of positive integers has a least element is the **Well-Ordering Principle** for the positive integers.

Proposition: Let n and N be two integers, with $m|N$. Then for any integer x

$$(x \% N) \% n = x \% n$$

Proof: Write $N = kn$ for some integer k , and let $x = Q \cdot N + R$ with $0 \leq R < |N|$. This R is the reduction of $x \bmod N$. Further, let $R = q \cdot n + r$ with $0 \leq r < |n|$. This r is the reduction of $R \bmod n$. Then

$$x = QN + R = Q(kn) + qn + r = (Qk + q) \cdot n + r$$

So r is also the reduction of x modulo m . *Done.*

5.3 Greatest common divisors, least common multiples

An integer d is a **common divisor** of a family of integers n_1, \dots, n_m if d divides each one of the integers n_i . An integer N is a **common multiple** of a family of integers n_1, \dots, n_m if N is a multiple of each of the integers n_i .

Theorem: Let m, n be integers, not both zero. Among all *common* divisors of m, n there is a unique one, call it d , so that for *every* other common divisor e of m, n we have $e|d$, and also $d > 0$. This divisor d is the *greatest common divisor* or **gcd** of m, n . The greatest common divisor of two integers m, n (not both zero) is the *least positive integer* of the form $xm + yn$ with $x, y \in \mathbf{Z}$.

Remark: The theorem gives a strange and possibly very counter-intuitive characterization of the greatest common divisor of two integers. However, it is this characterization which is necessary to *prove* things, *not* the more intuitive picture one might have of the *gcd* in terms of factorization into primes. A strange situation.

Remark: The greatest common divisor of m, n is denoted $gcd(m, n)$. Two integers are **relatively prime** or **coprime** if their greatest common divisor is 1. Also we may say that m is **prime to** n if they are relatively prime.

Proof: Let $D = x_0m + y_0n$ be the least positive integer expressible in the form $xm + yn$. First, we show that any divisor d of both m and n surely divides D . Write $m = m'd$ and $n = n'd$ with $m', n' \in \mathbf{Z}$. Then

$$D = x_0m + y_0n = x_0(m'd) + y_0(n'd) = (x_0m' + y_0n') \cdot d$$

which certainly presents D as a multiple of d .

On the other hand, apply the Division Algorithm to write $m = qD + r$ with $0 \leq r < D$. Then

$$0 \leq r = m - qD = m - q(x_0m + y_0n) = (1 - qx_0) \cdot m + (-y_0) \cdot n$$

That is, this r is also expressible as $x'm + y'n$ for integers x', y' . Since $r < D$, and since D is the smallest positive integer so expressible, it must be that $r = 0$. Therefore, $D|m$. Similarly, $D|n$. *Done.*

A companion or ‘dual’ notion concerning *multiples* instead of *divisors* is:

Corollary: Let m, n be integers, not both zero. Among all *common* multiples of m, n there is a unique one, call it N , so that for *every* other common multiple M of m, n we have $N|M$, and also $N > 0$. This multiple N is the *least common multiple* or **lcm** of m, n .

Remark: If we *already have* the prime factorizations of two numbers m, n , then we can easily find the greatest common divisor and least common multiple. Specifically, for each prime number p , the power of p dividing the *gcd* is the *minimum* of the powers of p dividing m and dividing n . Since this is true for each prime, we know the prime factorization of the greatest common divisor. For example,

$$gcd(2^3 3^5 5^2 11, 3^2 5^3 7^2 11^2) = 3^2 5^2 11$$

since 2^0 is the smaller of the two powers of 2 occurring, 3^2 is the smaller of the two powers of 3 occurring, 5^2 is the smaller of the two powers of 5 occurring, 7^0 is the smaller of the two powers of 7 occurring, and 11^1 is the smaller of the two powers of 11 occurring.

Similarly, the least common multiple is obtained by taking the *larger* of the two powers of each prime occurring in the factorizations of m, n .

However, we will see that this approach to computing greatest common divisors or least common multiples (by way of prime factorizations) is very inefficient.

5.4 Euclidean Algorithm

The **Euclidean Algorithm** is a very important and non-obvious systematic procedure to find the *greatest common divisor* d of two integers m, n , and *also* to find integers x, y so that

$$xm + yn = d$$

As we'll see just below, each step in the Euclidean Algorithm is an instance of the Division algorithm.

One important aspect of the Euclidean Algorithm is that it *avoids* factorization of integers into primes, and at the same time is a reasonably *fast* algorithm to accomplish its purpose. This is true at the level of hand calculations *and* for machine calculations, too.

Unlike the Division Algorithm, for which we didn't bother to describe the actual *procedure* but just the *outcome*, the Euclidean Algorithm needs description, which we do now, in examples.

To perform the Euclidean Algorithm for the two integers 513, 614:

$$614 - 1 \cdot 513 = 101 \quad (\text{reduction of } 614 \text{ mod } 513)$$

$$513 - 5 \cdot 101 = 8 \quad (\text{reduction of } 513 \text{ mod } 101)$$

$$101 - 12 \cdot 8 = 5 \quad (\text{reduction of } 101 \text{ mod } 8)$$

$$8 - 1 \cdot 5 = 3 \quad (\text{reduction of } 8 \text{ mod } 5)$$

$$5 - 1 \cdot 3 = 2 \quad (\text{reduction of } 5 \text{ mod } 3)$$

$$3 - 1 \cdot 2 = 1 \quad (\text{reduction of } 3 \text{ mod } 2)$$

Notice that the first step is reduction of the larger of the given numbers modulo the smaller of the two. The second step is reduction of the smaller of the two modulo the remainder from the first step. At each step, the 'modulus' of the previous step becomes the 'dividend' for the next step, and the 'remainder' from the previous step becomes the 'modulus' for the next step.

In this example, since we obtained a 1 as a remainder, we know that the greatest common divisor of 614 and 513 is just 1, that is, that 614, 513 are *relatively prime*. By the time we got close to the end, it could have been clear that we were going to get 1 as the gcd, but we carried out the procedure to the bitter end.

Notice that we did not need to find prime factorizations in order to use the Euclidean Algorithm to find the greatest common divisor. Since it turns out to be a time-consuming task to factor numbers into primes, this fact is worth something.

As another example, let's find the gcd of 1024 and 888:

$$1024 - 1 \cdot 888 = 136 \quad (\text{reduction of } 1024 \text{ mod } 888)$$

$$888 - 6 \cdot 136 = 72 \quad (\text{reduction of } 888 \text{ mod } 136)$$

$$136 - 1 \cdot 72 = 64 \quad (\text{reduction of } 136 \text{ mod } 72)$$

$$72 - 1 \cdot 64 = 8 \quad (\text{reduction of } 72 \text{ mod } 64)$$

$$64 - 8 \cdot 8 = 0 \quad (\text{reduction of } 64 \text{ mod } 8)$$

In this case, since we got a remainder 0, we must look at the remainder on the *previous* line: 8. The conclusion is that 8 is the greatest common divisor of 1024 and 888.

So far we've only seen how to find $\gcd(m, n)$. For small numbers we might feel that it's not terribly hard to do this just by factoring m, n into primes and comparing factorizations, as mentioned above. However, the problem of finding integers x, y so that

$$\gcd(m, n) = xm + yn$$

is much more of a hassle even for relatively small integers m, n .

The Euclidean Algorithm provides means to find these x, y with just a little more trouble, requiring that we have kept track of all the numbers occurring in the Euclidean Algorithm, and that we *run it backward*, as follows.

In the case of 614 and 513:

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 && (\text{last line of algorithm}) \\ &= 3 - 1 \cdot (5 - 1 \cdot 3) && (\text{replacing } 2 \text{ by its expression from the previous line}) \\ &= -1 \cdot 5 + 2 \cdot 3 && (\text{rearranging as sum of } 5\text{'s and } 3\text{'s}) \\ &= -1 \cdot 5 + 2 \cdot (8 - 1 \cdot 5) && (\text{replacing } 3 \text{ by its expression from the previous line}) \\ &= 2 \cdot 8 - 3 \cdot 5 && (\text{rearranging as sum of } 8\text{'s and } 5\text{'s}) \\ &= 2 \cdot 8 - 3 \cdot (101 - 12 \cdot 8) && (\text{replacing } 5 \text{ by its expression from the previous line}) \\ &= -3 \cdot 101 + 38 \cdot 8 && (\text{rearranging as sum of } 101\text{'s and } 8\text{'s}) \\ &= -3 \cdot 101 + 38 \cdot (513 - 5 \cdot 101) && (\text{replacing } 8 \text{ by its expression from the previous line}) \\ &= 38 \cdot 513 - 193 \cdot 101 && (\text{rearranging as sum of } 513\text{'s and } 101\text{'s}) \\ &= 38 \cdot 513 - 193 \cdot (614 - 513) && (\text{replacing } 101 \text{ by its expression from the previous line}) \\ &= 231 \cdot 513 - 193 \cdot 614 && (\text{rearranging as sum of } 614\text{'s and } 513\text{'s}) \end{aligned}$$

That is, we have achieved our goal: we now know that

$$1 = 231 \cdot 513 - 193 \cdot 614$$

In order to successfully execute this algorithm, it is important to keep track of which numbers are mere *coefficients*, and which are the numbers to be *replaced* by more complicated expressions coming from the earlier part of the algorithm. Thus, there is considerable reason to write it out as done just here, with the *coefficients first*, with the numbers to be substituted-for *second*.

5.5 Unique factorization: introduction

The fact that integers factor uniquely as products of primes is probably well-known to all of us from our experience with integers. And it is provably true. This a very special case of the unique factorization we'll prove later for *Euclidean rings*. In this subsection we'll just make a precise statement of facts.

Theorem: Unique Factorization Every integer n can be written in an *essentially unique* way as \pm a product of primes:

$$n = \pm p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$$

with positive integer exponents and distinct primes p_1, \dots, p_m .

Remark: The 'essentially unique' means that of course writing the product in a different order does not count as truly 'different'. The use of the word 'distinct' is typical of mathematics usage: it means 'no two of them are the same'. (This is a sharpening of the more colloquial use of 'different'.) The \pm in the theorem is necessary since n might be negative but primes numbers themselves are positive.

The proof of the theorem starts from the following key lemma, which may *feel* obvious, but is not.

Lemma: Let p be a prime number, and suppose that a and b are integers, with $p|(ab)$. Then either $p|a$ or $p|b$ (or both).

Proof: This proof is surely one of the least-expected arguments in elementary number theory! Suppose that $p|ab$ but $p \nmid a$, and show that $p|b$. Let $ab = mp$ for some integer m . Since p is prime and does not divide a , $\gcd(p, a) = 1$. Thus, there are integers s, t so that $sp + ta = 1$. Then

$$b = b \cdot 1 = b \cdot (sp + ta) = bsp + bta = bsp + tmp = p \cdot (bs + tm)$$

Visibly b is a multiple of p . ♣

Corollary: (of Lemma) If a prime p divides a product $a_1 a_2 \dots a_n$ then necessarily p divides at least one of the factors a_i .

5.6 Multiplicative inverses modulo m

This notion of "inverse" has no concrete connection to the elementary idea of inverse, but abstractly it is very similar. The Euclidean algorithm also gives an efficient method for computation of inverses modulo m .

A **multiplicative inverse mod m** of an integer N is another integer t so that $N \cdot t \% m = 1$. It is important to realize that this new notion of 'inverse' has no tangible relation to more elementary notions of 'inverse'.

For example, since $2 \cdot 3 = 6$ which reduces mod 5 to 1, we can say that 3 is a multiplicative inverse mod 5 to 2. This is *not* to say that ' $3 = \frac{1}{2}$ ' or ' $3 = 0.5$ ' or any such thing. As another example, 143 is a multiplicative inverse to 7 modulo 100, since $7 \times 143 = 1001$, which reduces mod 100 to 1. On the other hand, we can anticipate that, for example, 2 has no multiplicative inverse modulo 10, because any multiple $2 \times t$ is an *even* number, but all expressions $q \times 10 + 1$ are *odd*.

Theorem: Fix a non-zero modulus m . An integer x has a multiplicative inverse modulo m if and only if $\gcd(x, m) = 1$. If $\gcd(x, m) = 1$, let s, t be integers so that $sx + tm = 1$. Then s is a multiplicative inverse of x modulo m .

Remark: The Euclidean algorithm provides an efficient method to find expressions $\gcd(x, m) = sx + tm$, so thereby provides an efficient method to find multiplicative inverses.

Proof: If x has a multiplicative inverse y modulo m , then

$$xy = 1 + \ell m$$

for some integer ℓ . Rearranging, this is

$$1 = xy - \ell m$$

Thus, if $d|x$ and $d|m$ then $d|1$, from which follows that x and m are relatively prime.

On the other hand, suppose that $\gcd(x, m) = 1$. From above, we know that the *gcd* is expressible as

$$1 = \gcd(x, m) = sx + tm$$

for some $s, t \in \mathbf{Z}$. Rearranging this equation, we have

$$sx = 1 + (-t)m$$

which shows that $sx \equiv 1 \pmod{m}$. Thus, this s is a multiplicative inverse of x modulo m . ♣

5.7 Integers modulo m

If two integers x, y differ by a multiple of a non-zero integer m , we say that x is **congruent to y modulo m** , written

$$x \equiv y \pmod{m}$$

Any relation such as the latter is called a **congruence** modulo m , and m is the **modulus**.

Equivalently, $x \equiv y \pmod{m}$ if and only if $m|(x - y)$.

The idea of thinking of *integers modulo m* as necessarily having something to do with *reduction modulo m* is seductive, but is a trap. If for no other reason than this, a somewhat richer vocabulary of concepts is necessary in order to discuss more sophisticated things.

For example, $3 \equiv 18 \pmod{5}$ because $5|(18 - 3)$. Yes, indeed, this is ‘just’ a different way of writing a divisibility assertion. But this notation (due to Gauss, almost 200 years ago) is meant to cause us to think of *congruence* as a variant of *equality*, with comparable features. That congruences really do have properties similar to equality requires some proof, even though the proofs are not so hard. In giving the statements of these properties the corresponding terminology is also introduced.

Proposition: For a fixed integer m , congruence modulo m is an *equivalence relation*. That is,

- *Reflexivity:* Always $x \equiv x \pmod{m}$ for any x .
- *Symmetry:* If $x \equiv y \pmod{m}$ then $y \equiv x \pmod{m}$.
- *Transitivity:* If $x \equiv y \pmod{m}$ and $y \equiv z \pmod{m}$ then $x \equiv z \pmod{m}$.

Proof: Since $x - x = 0$ and always $m|0$, we have reflexivity. If $m|(x - y)$ then $m|(y - x)$ since $y - x = -(x - y)$. Thus, we have symmetry. Suppose that $m|(x - y)$ and $m|(y - z)$. Then there are integers k, ℓ so that $mk = x - y$ and $m\ell = y - z$. Then

$$x - z = (x - y) + (y - z) = mk + m\ell = m \cdot (k + \ell)$$

This proves the transitivity. *Done.*

For any integer x , the collection of all integers y congruent to x modulo m is the **congruence class** of x modulo m . This is also called the **residue class** of x modulo m , or **equivalence class** of x with respect to the equivalence relation of congruence modulo m .

The **integers mod m** is the collection of *congruence classes* of integers with respect to the equivalence relation *congruence modulo m* . It is denoted \mathbf{Z}/m (or sometimes \mathbf{Z}_m).

Given an integer x and a modulus m , the equivalence class

$$\{y \in \mathbf{Z} : y \equiv x \pmod{m}\}$$

of x modulo m is often denoted \bar{x} , and is also called the **congruence class** or **residue class** of x mod m . On other occasions, the bar notation is not used at all, so that $x\text{-mod-}m$ may be written simply as ‘ x ’ with only the *context* to make clear that this means $x\text{-mod-}m$ and not the integer x .

Thus, for example, modulo 12 we have

$$\bar{0} = \overline{12} = \overline{-12} = \overline{2400}$$

$$\bar{7} = \overline{7} = \overline{-5} = \overline{2407}$$

$$\bar{1} = \overline{13} = \overline{-11} = \overline{2401}$$

or, equivalently,

$$0\text{-mod-}12 = 12\text{-mod-}12 = -12\text{-mod-}12 = 2400\text{-mod-}12$$

$$7\text{-mod-}12 = 7\text{-mod-}12 = -5\text{-mod-}12 = 2407\text{-mod-}12$$

$$1\text{-mod-}12 = 13\text{-mod-}12 = -11\text{-mod-}12 = 2401\text{-mod-}12$$

Remark: There is one traditionally popular collection of representatives for the equivalence classes modulo m , namely

$$\{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-2}, \overline{m-1}\}$$

In fact, some flawed sources *define* integers-mod- m as being this set of things, but this is too naive an understanding of what kind of thing integers-mod- m really is. We should distinguish the set of integers *reduced mod m* (which really is $\{0, 1, 2, \dots, m-1\}$!) from the set of integers *modulo m* , which is the set of equivalence classes of integers modulo m . The latter is a more abstract object.

So while it is certainly true that (for example)

$$\mathbf{Z}/3 = \{\bar{0}, \bar{1}, \bar{2}\}$$

it is also true that

$$\mathbf{Z}/3 = \{\overline{10}, \overline{31}, \bar{-1}\}$$

and that there are many other ways of describing it as well.

Again: \mathbf{Z}/n is *not* the set of integers $\{0, 1, 2, 3, \dots, m-1\}$. Rather, \mathbf{Z}/n is the set of *equivalence classes* modulo m . The set $\{0, 1, 2, 3, \dots, m-1\}$ is the set of integers *reduced modulo m* (for which there is no special symbol). Still, we do have:

Proposition: Fix two integers x, x' . Let $x = qm + r$ and $x' = q'm + r'$ with integers q, q', r, r' and $0 \leq r < |m|$ and $0 \leq r' < |m'|$. Then $x \equiv x' \pmod{m}$ if and only if $r \equiv r' \pmod{m}$.

Proof: If $x \equiv x' \pmod{m}$ then there is an integer k so that $x' = x + km$. Then

$$\begin{aligned} r' &= x' - q'm = (x + km) - q'm = x + m \cdot (k - q') = qm + r + m \cdot (k - q') \\ &= r + m \cdot (q + k - q') \end{aligned}$$

This proves that $r \equiv r' \pmod{m}$. The opposite direction of argument is similar. *Done.*

Beyond being just an equivalence relation, congruences behave very nicely with respect to the basic arithmetic operations of addition, subtraction, and multiplication:

Proposition: For fixed modulus m , If $x \equiv x'$ then for all y

$$x + y \equiv x' + y \pmod{m}$$

$$xy \equiv x'y \pmod{m}$$

In fact, if $y \equiv y'$, then

$$x + y \equiv x' + y' \pmod{m}$$

$$x \cdot y \equiv x' \cdot y' \pmod{m}$$

Proof: It suffices to prove only the more general assertions. Since $x' \equiv x \pmod{m}$, $m|(x' - x)$, so there is an integer k so that $mk = x' - x$. That is, we have $x' = x + mk$. Similarly, we have $y' = y + \ell m$ for integer ℓ . Then

$$x' + y' = (x + mk) + (y + \ell m) = x + y + m \cdot (k + \ell)$$

Thus, $x' + y' \equiv x + y \pmod{m}$. And

$$x' \cdot y' = (x + mk) \cdot (y + \ell m) = x \cdot y + x\ell m + mky + mk \cdot \ell m = x \cdot y + m \cdot (k\ell + m\ell k)$$

Thus, $x'y' \equiv xy \pmod{m}$. *Done.*

As a corollary of this last proposition, congruences immediately *inherit* some properties from ordinary arithmetic, simply because $x = y$ implies $x \equiv y \pmod{m}$:

- *Distributivity:* $x(y + z) \equiv xy + xz \pmod{m}$
- *Associativity of addition:* $(x + y) + z \equiv x + (y + z) \pmod{m}$
- *Associativity of multiplication:* $(xy)z \equiv x(yz) \pmod{m}$
- *Property of 1:* $1 \cdot x \equiv x \cdot 1 \equiv x \pmod{m}$
- *Property of 0:* $0 + x \equiv x + 0 \equiv x \pmod{m}$

We should feel reassured by these observations that we can do arithmetic ‘mod m ’ without anything messing up. As a matter of notation, we write

$$\mathbf{Z}/m$$

for **the integers mod m** , viewing two integers x, y as ‘the same’ if $x \equiv y \pmod{m}$. Thus, there are only m ‘things’ in \mathbf{Z}/m , since there are only m possibilities for what an integer can be congruent to mod m . Very often, a person thinks of $0, 1, 2, \dots, m - 2, m - 1$ as being the ‘things’ in \mathbf{Z}/m , but this is not quite good enough for *all* purposes.

And there are some more practical observations which also deserve emphasis:

- $m \equiv 0 \pmod{m}$, and generally $km \equiv 0 \pmod{m}$ for any integer k .
- $x + (-x) \equiv 0 \pmod{m}$
- $x \pm m \equiv x \pmod{m}$, and generally $x + km \equiv x \pmod{m}$ for any integer k

Note that in all this discussion we only look at one modulus m at a time.

Corollary: For a fixed modulus m in each residue class there is exactly one integer which is *reduced mod m* . Therefore, $x \equiv y \pmod{m}$ if and only if x and y have the same *reduction mod m* , that is, have the same remainder when divided by m as in the Division/Reduction Algorithm.

Proof: Fix an integer x . Invoking the Reduction algorithm, there is a *unique* $0 \leq r < |m|$ and an integer q so that $x = qm + r$. Then $x - r = qm$ is divisible by m , so x and r are in the same residue class. Since r is reduced, this proves that there is at least one reduced representative for each residue class.

On the other hand, (reproving the uniqueness part of the Reduction Algorithm!), suppose that $x \equiv r'$ for r' in the range $0 \leq r' < |m|$. If $0 \leq r < r'$, then

$$0 < r' - r = (r' - x) - (r - x)$$

is multiple of m . Yet also $0 < r' - r \leq r' < |m|$. But a multiple of m cannot be > 0 and $< |m|$, so it cannot be that $0 \leq r < r'$. Or, supposing that $0 \leq r' < r$, by a symmetrical argument we would again reach a contradiction. Thus, $r = r'$. This proves the uniqueness. *Done.*

Corollary: Fix a modulus m , and integers x and y . For brevity write

$$x \% m$$

for x reduced modulo m . Then

$$(x + y) \% m = ((x \% m) + (y \% m)) \% m$$

and

$$(x \cdot y) \% m = ((x \% m) \cdot (y \% m)) \% m$$

Proof: The residue class of $x' = (x \% m)$ is the same as the residue class of x itself. Therefore, modulo m , we have

$$((x \% m) + (y \% m)) \% m \equiv (x \% m) + (y \% m) \equiv x + y$$

since we proved that $x' \equiv x$ and $y' \equiv y$ gives $x' + y' \equiv x + y$. Further, similarly,

$$x + y \equiv (x + y) \% m$$

Thus, by transitivity,

$$((x \% m) + (y \% m)) \% m \equiv (x + y) \% m$$

The same argument works for multiplication. *Done.*

One would correctly get the impression that all properties of congruences follow from properties of ordinary equality together with properties of elementary arithmetic.

We return again to *multiplicative inverses modulo m* . That is, to find a multiplicative inverse mod m for a , we want to solve for x in the equation

$$ax \equiv 1 \pmod{m}$$

where the integer a is given. Unless $a = \pm 1$ the solution $x = \frac{1}{a}$ of the equation $ax = 1$ is *not* an integer. But that's not what's going on here. Rather, recall that if $\gcd(a, m) = 1$ then there are integers x, y so that

$$ax + ym = \gcd(a, m) = 1$$

Then $ax - 1 = ym$ is a multiple of m , so with this value of x

$$ax \equiv 1 \pmod{m}$$

Unless $a = \pm 1$, this x can't possibly be $\frac{1}{a}$, if only because $\frac{1}{a}$ is not an integer. We are doing something new.

Recall that we *did* prove that a has a multiplicative inverse if and only if $\gcd(a, m) = 1$, in which case the Euclidean Algorithm is an effective means to actually *find* the inverse.

In light of the last observation, we have a separate notation for the integers-mod- m which are relatively prime to m and hence have inverses:

$$\mathbf{Z}/m^\times$$

The superscript is not an 'x', but is a 'times', making a reference to multiplication and multiplicative inverses, but mod m .

Proposition: The product xy of two integers x and y both prime to m is again prime to m .

Proof: One way to think about this would be in terms of *prime factorizations*, but let's do without that. Rather, let's use the fact that the \gcd of two integers a, b can be expressed as

$$\gcd(a, b) = sa + tb$$

for some integers s, t . Thus, there are integers a, b, c, d so that

$$1 = ax + bm \quad 1 = cy + dm$$

Then

$$1 = 1 \cdot 1 = (ax + bm)(cy + dm) = (ac)(xy) + (bcy + axd + bdm)m$$

Thus, 1 is expressible in the form $A(xy) + Bm$, so (by the sharp form of this principle!) necessarily xy and m are relatively prime. *Done.*

So in the batch of things denoted \mathbf{Z}/m^\times we can multiply and take inverses (so, effectively, divide).

#5.30 Prove directly, from the very definition of divisibility, that if $d|x$ and $d|y$ then $d|(x - y)$ and $d|(x + y)$.

#5.31 Observe that 121, 1331, and 14641 cannot be prime, without computation.

#5.32 Find the greatest common divisor of 6, 10, 15.

#5.33 Find the least common multiple of 6, 10, 15.

#5.34 Find the greatest common divisor of 2, 4, 8, 16, 32, 64, 128.

#5.35 Find the least common multiple of 2, 4, 8, 16, 32, 64, 128.

#5.36 Show that for any integer n if $d|n$ and $d|(n + 2)$ then $d|2$.

#5.37 Show that for any integer n the two integers n and $n + 1$ are invariably relatively prime.

#5.38 Show that for any integer n exactly one of $n, n + 2, n + 4$ is divisible by 3. In particular, except for 3, 5, 7, there are no triples of primes occurring in the pattern $n, n + 2, n + 4$.

#5.39 Show that for any integer n , the integers n and $n^2 + 1$ are relatively prime.

#5.40 Prove that for any two integers m, n , the least common multiple $\text{lcm}(m, n)$ exists, and $\text{lcm}(m, n) = m \cdot n / \gcd(m, n)$.

#5.41 Find the reduction mod 99 of 1000.

#5.42 Find the reduction mod 88 of -1000.

#5.43 Prove that the reduction mod 10 of a positive integer N is simply the ones' place digit of N in decimal notation.

#5.44 Prove that the reduction mod 100 of a positive integer N is the two-digit number made up of the tens' and ones' place digits of N .

#5.45 Let m be any non-zero integer. Prove that the reduction mod $-m$ of N is the same as the reduction mod m of N .

#5.46 Prove in general that if r is the reduction of N mod m , and if $r \neq 0$, then $m - r$ is the reduction of $-N$ mod m .

#5.47 Find $\gcd(1236, 4323)$ and express it in the form $1236x + 4323y$ for some integers x, y , by hand computation.

#5.48 Find $\gcd(12367, 24983)$, and express it in the form $12367x + 24983y$, by hand computation.

#5.49 Find a proper factor of 111, 111, 111, 111, 111 without using a calculator.

#5.50 Prove/observe that the one's-place digit of a decimal number *cannot* be sufficient information (by itself) to determine whether the number is divisible by 3, or by 7.

#5.51 Explain why $2^m + 1$ cannot possibly be a prime number unless m is a power of 2. (If it *is* prime then it's called a **Fermat prime**.)

#5.52 Explain why $2^m - 1$ cannot possibly be a prime number unless m is prime. (If it *is* prime then it's called a **Mersenne prime**.)

#5.53 How many elements does the set \mathbf{Z}/n have?

#5.54 How many elements does the set $\mathbf{Z}/30^\times$ have?

#5.55 Find the multiplicative inverse of 3 modulo 100.

#5.56 Find the multiplicative inverse of 1001 modulo 1234.

6. Unique factorization into primes

We now can prove the *unique factorization of integers into primes*. This very possibly may already seem “intuitively true”, since after all our experience with small integers bears witness to the truth of the assertion. And it is true, after all. But it is worth paying attention to *how* such a thing can be proven, especially since we will later want to *try* to prove unique factorization for fancier kinds of “numbers”, for which our intuition is not adequate. Since it is *not* true in general that “all kinds” of numbers can be factored uniquely into primes, we must be alert.

While we’re here, we also give a formula for Euler’s *phi*-function $\varphi(n)$, whose definition

$$\varphi(n) = \text{number of integers } i \text{ in the range } 0 \leq i \leq n \text{ relatively prime to } n$$

We also look at the most naive **primality test**, as well as the most naive algorithm to obtain the **factorization** of an integer into primes. To obtain the list of all primes less than a given bound, we mention **Eratoshenes’ sieve**, which is reasonably efficient for what it does.

Also, we can take this occasion to review some algebraic identities which occasionally provide shortcuts in the otherwise potentially laborious task of ascertaining whether a given number is prime, and/or factoring it into primes.

Theorem: Unique Factorization Every integer n can be written in an *essentially unique* way as \pm a product of primes:

$$n = \pm p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$$

with positive integer exponents and distinct primes p_1, \dots, p_m .

Remark: The ‘essentially unique’ means that of course writing the product in a different order does not count as truly ‘different’. The use of the word ‘distinct’ is typical of mathematics usage: it means ‘no two of them are the same’. (This is a sharpening of the more colloquial use of ‘different’.) The \pm in the theorem is necessary since n might be negative but primes numbers themselves are positive.

Corollary: Let N be a positive integer factored into primes as

$$N = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$$

where p_1, \dots, p_n are distinct primes, and the exponents e_i are all non-negative integers. Then the Euler *phi*-function of N has the value

$$\varphi(N) = (p_1 - 1)p_1^{e_1 - 1} (p_2 - 1)p_2^{e_2 - 1} \dots (p_n - 1)p_n^{e_n - 1}$$

The proof of the theorem starts from the following key lemma, which may *feel* obvious, but is not.

Lemma: Let p be a prime number, and suppose that a and b are integers, with $p|(ab)$. Then either $p|a$ or $p|b$, or both.

Proof: (of Lemma) If $p|a$ we are done. So suppose that p does not divide a . Then the *greatest* common divisor $\gcd(p, a)$ can’t be p . But this greatest common divisor is also a divisor of p , and is positive. Since p is *prime*, the only positive divisor of p other than p itself is just 1. Therefore, $\gcd(p, a) = 1$. We saw that there exist integers x, y so that $xp + ya = 1$.

Since $p|(ab)$, we can write $ab = hp$ for some integer h .

$$b = b \cdot 1 = b \cdot (xp + ya) = bxp + yba = (bx + yh) \cdot p$$

This shows that b is a multiple of p . *Done.*

Corollary: (of Lemma) If a prime p divides a product $a_1 a_2 \dots a_n$ then necessarily p divides at least one of the factors a_i .

Proof: (of Corollary) This is by induction on n . The Lemma is the assertion for $n = 2$. Suppose $p|(a_1 \dots a_n)$. Then write the latter product as

$$a_1 \dots a_n = (a_1 \dots a_{n-1}) \cdot a_n$$

By the lemma, either p divides a_n or p divides $a_1 a_2 \dots a_{n-1}$. If $p|a_n$ we are done. If not, then $p|(a_1 \dots a_{n-1})$. By induction, this implies that p divides one of the factors a_1, a_2, \dots, a_{n-1} . Altogether, we conclude that in any case p divides one of the factors a_1, \dots, a_n . *Done.*

Proof: (of Theorem) First we prove that for every integer there *exists* a factorization, and then that it is *unique*. It certainly suffices to treat only factorizations of *positive* integers, since factorizations for $-n$ and n are obviously related.

For *existence*, suppose that some integer $n > 1$ did *not* have a factorization into primes. Then n cannot be prime itself, or just " $n = n$ " is a factorization into primes. Therefore n has a proper factorization $n = xy$ with $x, y > 0$. Since the factorization is *proper*, both x and y are strictly smaller than n . Thus, x and y both can be factored into primes. Putting together the two factorizations gives the factorization of n . This contradicts the assumption that there exist any integers lacking prime factorizations.

Now prove *uniqueness*. Suppose we have

$$q_1^{e_1} \dots q_m^{e_m} = N = p_1^{f_1} \dots p_n^{f_n}$$

where (without loss of generality)

$$q_1 < q_2 < \dots < q_m$$

are primes, and also

$$p_1 < p_2 < \dots < p_n$$

are all primes. And the exponents e_i and f_i are positive integers. We must show that $m = n$, $q_i = p_i$ for all i , and $e_i = f_i$ for all i .

Since q_1 divides the left-hand side of the equality, it must divide the right-hand side. Therefore, by the corollary to the lemma just above, q_1 must divide one of the factors on the right-hand side. So q_1 must divide some p_i . Since p_i is prime, it must be that $q_1 = p_i$.

We claim that $i = 1$. Indeed, if $i > 1$ then $p_1 < p_i$. And p_1 divides the left-hand side, so divides one of the q_j , so is equal to some q_j . But then $q_j \geq q_1 = p_i > p_1$, which is impossible. Therefore, $q_1 = p_1$.

Further, by dividing through by e_1 factors $q_1 = p_1$, we see that the corresponding exponents e_1 and f_1 must also be equal.

The rest of the argument about uniqueness is by induction on N . First, 1 has a unique factorization (of sorts), namely the *empty* product. In any case, since 2 is prime it has the factorization $2 = 2$. This begins the induction. Suppose that all integers $N' < N$ have unique factorizations into primes (and prove that N likewise has a unique factorization).

From the equation

$$q_1^{e_1} \dots q_m^{e_m} = N = p_1^{f_1} \dots p_n^{f_n}$$

by dividing by $q_1^{e_1} = p_1^{f_1}$ we obtain

$$q_2^{e_2} \dots q_m^{e_m} = \frac{N}{q_1^{e_1}} = p_2^{f_2} \dots p_n^{f_n}$$

We had suppose that all the exponents e_i were positive, so $N/q_1^{e_1} < N$. Thus, by induction, $N/q_1^{e_1}$ has unique factorization, and we conclude that all the remaining factors must match up. This finishes the proof of the unique factorization theorem. *Done.*

Now we prove the corollary, giving the formula for Euler's *phi*-function:

$$\varphi(N) = (p_1 - 1)p_1^{e_1 - 1} (p_2 - 1)p_2^{e_2 - 1} \dots (p_n - 1)p_n^{e_n - 1}$$

where $n = p_1^{e_1} \dots p_n^{e_n}$ is the factorization into *distinct* prime factors p_i , and all exponents are positive integers. The argument is by *counting*: we'll count the number of numbers x in the range from 0 through $N - 1$ which *do* have a common factor with N , and subtract. And, by unique factorization, if x has a common factor with N then it has a common *prime* factor with N . There are exactly N/p_i numbers divisible by p_i , so we would be tempted to say that the number of numbers in that range with *no* common factor with N would be

$$N - \frac{N}{p_1} - \frac{N}{p_2} - \dots - \frac{N}{p_n}$$

However, this is not correct in general: we have accounted for numbers divisible by two *different* p_i 's *twice*, so we should add back in all the expressions $N/p_i p_j$ with $i \neq j$. But then we've added back in too many things, and have to *subtract* all the expressions $M/p_i p_j p_k$ with i, j, k distinct. And so on:

$$\begin{aligned} \varphi(N) &= N - \sum_i \frac{N}{p_i} + \sum_{i \neq j} \frac{N}{p_i p_j} - \sum_{i, j, k \text{ distinct}} \frac{N}{p_i p_j p_k} + \dots \\ &= N \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_n}\right) \\ &= p_1^{e_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{e_2} \left(1 - \frac{1}{p_2}\right) \dots p_n^{e_n} \left(1 - \frac{1}{p_n}\right) \\ &= (p_1 - 1)p_1^{e_1 - 1} (p_2 - 1)p_2^{e_2 - 1} \dots (p_n - 1)p_n^{e_n - 1} \end{aligned}$$

This is the desired formula. *Done.*

The most obvious (but not most efficient) means to *obtain* the **prime factorization** and simultaneously to **test primality** of a positive integer N is as follows. Attempt division by integers $d = 2, 3, 4, 5, 6, 7, \dots \leq \sqrt{N}$ until either the smallest divisor $d_1 > 1$ of N is found, or it is determined that N has no proper divisors $\leq \sqrt{N}$. In the latter case, N is prime. In the former case, attempt division by integers $d = d_1, d_1 + 1, d_1 + 2, \dots \leq \sqrt{N/d_1}$ until either the smallest divisor $d_2 > 1$ of N/d_1 is found, or it is determined that N/d_1 has no proper divisors $\leq \sqrt{N/d_1}$. In the latter case, N/d_1 is prime. In the former case, attempt division by integers $d = d_2, d_2 + 1, d_2 + 2, \dots \leq \sqrt{N/d_1 d_2}$ until either the smallest divisor $d_3 > 1$ of $N/d_1 d_2$ is found, or it is determined that $N/d_1 d_2$ has no proper divisors $\leq \sqrt{N/d_1 d_2}$. In the latter case $N/d_1 d_2$ is prime. In the former case...

This *recursive* procedure ends when some $N/d_1 d_2 \dots d_m$ is prime. At the same time, if N has no divisor d in the range $1 < d < \sqrt{N}$ then N is prime.

Remark: It is possible to make the procedure slightly more economical in an obvious way: in attempting division by d in the manner indicated, there is no reason to use non-primes, since if $d = ab$ with $a, b > 1$, then we would already have detected divisibility by both a and b earlier and divided out by them. On the other hand, the effort required to identify all the non-primes d may be more effort than it is worth.

Some sort of compromise approach is reasonable: for example, there is no reason to attempt division by *even* numbers other than 2, nor by numbers bigger than 5 other than 5 (nor numbers divisible by 10). The point is that for integers represented as decimals, divisibility by 2 or 5 (or 10) is very easy to identify.

Addressing a slightly different question, we might wish to find all primes less than a given bound N . A reasonable procedure for this is **Eratosthenes' Sieve**, described as follows. List all the integers from 2 through N .

- Starting with $2 + 2$, mark every 2nd integer on the list. (This marks all even numbers bigger than 2).
- The next integer (after 2) on the list which hasn't been marked is 3. Starting with $3 + 3$, mark every 3rd integer (counting those *already* marked). (This marks all multiples of 3 bigger than 3 itself.)
- The next integer (after 3) on the list which hasn't been marked is 5. Starting with $5 + 5$, mark every 5th integer (counting those *already* marked). (This marks all multiples of 5 bigger than 5 itself.)
- ...
- Take the *next* integer n on the list which has not yet been crossed-off. This n is **prime**. Starting with $n + n$, cross off every n^{th} integer (counting those *already* marked). (This marks all multiples of n bigger than n itself).
- ...
- Stop when you've marked all multiples of the largest prime less than \sqrt{N} .

For example, looking at the list of integers from 2 through 31 and executing this procedure, we first have the list

2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31

Marking multiples of 2 after 2 itself gives

2	3	4*	5	6*	7	8*	9	10*	11
12*	13	14*	15	16*	17	18*	19	20*	21
22*	23	24*	25	26*	27	28*	29	30*	31

Marking multiples of 3 after 3 itself gives

2	3	4*	5	6*	7	8*	9*	10*	11
12*	13	14*	15*	16*	17	18*	19	20*	21*
22*	23	24*	25	26*	27*	28*	29	30*	31

Marking multiples of 5 after 5 itself gives

2	3	4*	5*	6*	7	8*	9*	10*	11
12*	13	14*	15*	16*	17	18*	19	20*	21*
22*	23	24*	25*	26*	27*	28*	29	30*	31

By this point, the next unmarked integer is 7, which is larger than $\sqrt{31}$, so all the integers in the list unmarked by this point are *prime*.

There are **standard identities** which are useful in anticipating factorization of special polynomials and special forms of numbers:

$$\begin{aligned}
 x^2 - y^2 &= (x - y)(x + y) \\
 x^3 - y^3 &= (x - y)(x^2 + xy + y^2) & x^3 + y^3 &= (x + y)(x^2 - xy + y^2) \\
 x^4 - y^4 &= (x - y)(x^3 + x^2y + xy^2 + y^3) \\
 x^5 - y^5 &= (x - y)(x^4 + x^3y + x^2y^2 + xy^3 + y^4)
 \end{aligned}$$

$$x^5 + y^5 = (x + y)(x^4 - x^3y + x^2y^2 - xy^3 + y^4)$$

and so on. Note that for *odd* exponents there are *two* identities while for *even* exponents there is just *one*.

Thus, for example, we might be curious whether there are infinitely-many primes of the form $n^3 - 1$ for integers n . To address this, use

$$n^3 - 1 = (n - 1) \cdot (n^2 + n + 1)$$

Therefore, *if* both factors $n - 1$ and $n^2 + n + 1$ fall strictly between 1 and $n^3 - 1$, then this is a proper factorization of $n^3 - 1$, so $n^3 - 1$ could not be prime. In fact, it suffices to show that *one* of the factors is both > 1 and $< n^3 - 1$. Note that for $n = 2$ the expression $n^3 - 1$ has value 7, which *is* prime, so we'd better not try to prove that this expression is *never* prime.

For $n > 2$ certainly $n - 1 > 2 - 1 = 1$. This is one comparison. On the other hand, also for $n > 2$,

$$n - 1 < 2 \cdot 2 \cdot n - 1 < n \cdot n \cdot n - 1$$

Thus, $0 < n - 1 < n^3 - 1$ if $n > 2$. This shows that $n^3 - 1$ is *never* prime for $n > 2$.

One special algebraic form for numbers, which was historically of recreational interest, but is now also of practical interest, is $2^n - 1$. If such a number *is* prime, then it is called a **Mersenne prime**. It is not known whether or not there are infinitely-many Mersenne primes.

Another special form is $2^m + 1$. If such a number *is* prime, it is called a **Fermat prime**. It is not known whether there are infinitely-many primes of this form. Fermat evidently thought that every expression

$$2^{2^n} + 1$$

might be prime, but this was disproved by Euler about 100 years later.

#6.57 Factor the integers 1028 and 2057 into primes.

#6.58 Find a proper factor of 111, 111, 111, 111, 111 without using a calculator.

#6.59 Find a proper factor of 101, 010, 101, 010, 101 without using a calculator.

#6.60 Prove/observe that the one's-place digit of a decimal number *cannot* is not sufficient information (by itself) to determine whether the number is divisible by 3, or by 7.

#6.61 Explain why $n^2 - 1$ cannot be prime for *any* $n > 2$.

#6.62 Explain why $3^n - 1$ cannot possibly be a prime number if $n > 1$.

#6.63 Explain why $2^m + 1$ cannot possibly be a prime number unless m is a power of 2.

#6.64 While we mostly know that $x^2 - y^2$ has a factorization, that $x^3 - y^3$ has a factorization, that $x^3 + y^3$ has, and so on, there is a factorization that seldom appears in 'high school': $x^4 + 4y^4$ has a factorization into two quadratic pieces, each with 3 terms! Find this factorization. *Hint:*

$$x^4 + 4y^4 = (x^4 + 4x^2y^2 + 4y^4) - 4x^2y^2$$

#6.65 Can $n^4 + 4$ be a prime if the integer n is bigger than 1?

#6.66 Factor $x^6 - y^6$ in two different ways.

#6.67 (*) *Euclid's proof of the infinitude of primes* Suppose there were only finitely-many primes p_1, p_2, \dots, p_n . Consider the number $N = 2p_1 \dots p_n + 1$. Show that none of the p_i can divide N . Conclude that there must be some other prime than those on this list, contradiction. ■

7. (*) Prime Numbers

- Euclid's Theorem: infinitude of primes
 - The Prime Number Theorem
 - Chebycheff's Theorem
 - Sharpest known asymptotics
 - The Riemann Hypothesis
-

7.1 Euclid's Theorem: infinitude of primes

Our experience probably already suggested that integers have unique factorization into primes, but it is less intuitive that there are *infinitely many primes*. Euclid's 2000-year-old proof of this is not only ingenious, but also is a good example of an indirect proof ("by contradiction").

For this discussion we grant that integers have *unique factorizations* into primes. (This is a special case of our later result that *all Euclidean rings have unique factorization*.)

Theorem: (*Euclid*) There are infinitely-many prime numbers.

Proof: This is a proof by contradiction. Suppose that there were only finitely many primes. Then we could list *all* of them: p_1, \dots, p_n . Then consider the number

$$N = p_1 \cdot p_2 \cdot \dots \cdot p_{n-1} \cdot p_n + 1$$

That is, N is the product of all the primes, plus 1. Since $N > 1$, and since N has a factorization into primes, we can say that there is a prime p dividing N . Then p cannot be in the list p_1, \dots, p_n , since if it *were* in that list, then p would divide

$$N - (p_1 \dots p_n) = 1$$

which it does not. But the fact that p is not on the list contradicts the hypothesis that we had listed them all. That is, assuming that there were only finitely-many primes leads to a contradiction. Thus, there are infinitely-many primes. ♣

Note that this gives no substantial idea of what integers are or are not primes, nor "how many" primes there may be.

7.2 The Prime Number Theorem

Around 1800 Gauss and Legendre had made conjectures about the distribution of prime numbers, from looking at lists of primes, but were unable to prove anything very precise. It was not until 1896 that Hadamard and de la Vallée-Poussin independently proved the result described just below.

The standard counting function for primes is

$$\pi(x) = \text{number of primes less than } x$$

We use the standard notation that

$$f(x) \sim g(x)$$

means

$$\lim_{x \rightarrow +\infty} \frac{f(x)}{g(x)} = 1$$

Prime Number Theorem: As $x \rightarrow +\infty$

$$\pi(x) \sim \frac{x}{\ln x}$$

The proof of this is a bit difficult.

7.3 Chebycheff's Proof

In 1851 Chebycheff made a breakthrough toward proving the Prime Number Theorem. Although what he proved was weaker than the conjectured result, it was the first real progress beyond collecting statistics and making lists. His proof is more-or-less accessible in terms of things we know, so we'll do it here:

Theorem: (*Chebycheff*) There are positive constants c and C so that eventually (for large-enough x)

$$c \cdot \frac{x}{\ln x} \leq \pi(x) \leq C \cdot \frac{x}{\ln x}$$

Proof: We need to define standard auxiliary functions

$$\theta(x) = \sum_{p \text{ prime: } p < x} \ln p$$

$$\psi(x) = \sum_{p \text{ prime, } k \in \mathbf{Z}: p^k < x} \ln p$$

That is, in words, $\theta(x)$ is the sum of the natural logarithms of all primes less than x , and $\psi(x)$ is the sum of $\ln p$ for every *prime power* p^k less than x . The easiest estimates arise in terms of θ and ψ , so at the end we will return to see what these say about the prime-counting function π . The first thing necessary is to see that, for purposes of our asymptotic estimates, θ and ψ are not far apart. After that come two rather clever lemmas due to Chebycheff.

Lemma:

$$0 \leq \psi(x) - \theta(x) \leq x^{1/2}(\ln x)^2$$

(Proof left to the reader: there's nothing delicate about this comparison!)

Lemma: (*Chebycheff*) $\theta(x) = O(x)$.

Proof of Lemma: For $m = 2^e$ with positive integer e , consider the binomial coefficient

$$N = \binom{m}{m/2}$$

Since

$$2^m = (1 + 1)^m = \sum_{0 \leq k \leq m} \binom{m}{k} 1^{m-k} 1^k = \sum_{0 \leq k \leq m} \binom{m}{k}$$

it is clear that $\binom{m}{m/2}$ is a *positive integer*, and is less than 2^m . On the other hand, from the expression

$$\binom{m}{m/2} = \frac{m!}{(m/2)! (m/2)!}$$

we can see that each prime p in the range $\frac{m}{2} < p \leq m$ divides $\binom{m}{m/2}$. Thus,

$$\prod_{(m/2) < p \leq m} p \leq \binom{m}{m/2}$$

The natural logarithm function is **monotone increasing**, meaning that $x < y$ implies $\ln(x) < \ln(y)$. Therefore, taking natural logarithms of both sides of the last displayed inequality, we have

$$\theta(m) - \theta(m/2) \leq m \ln 2$$

That is,

$$\theta(2^e) - \theta(2^{e-1}) \leq m \ln 2 = 2^e \ln 2$$

Therefore, applying this repeatedly, we have

$$\begin{aligned} \theta(2^e) &= (\theta(2^e) - \theta(2^{e-1})) + \theta(2^{e-1}) \\ &\leq 2^e \ln 2 + (\theta(2^{e-1}) - \theta(2^{e-2})) + \theta(2^{e-2}) \\ &\leq 2^e \ln 2 + 2^{e-1} \ln 2 + \theta(2^{e-2}) \\ &\leq 2^e \ln 2 + 2^{e-1} \ln 2 + 2^{e-2} \ln 2 + \theta(2^{e-3}) \end{aligned}$$

which, by repeating further, is

$$\begin{aligned} &\leq 2^e \ln 2 + 2^{e-1} \ln 2 + 2^{e-2} \ln 2 + \dots + 2^1 \ln 2 + \ln 2 \\ &= 2^{e+1} \ln 2 - 1 \leq 2^{e+1} \ln 2 \end{aligned}$$

So for $2^{e-1} \leq x \leq 2^e$, we have

$$\theta(x) \leq \theta(2^e) = 2^{e+1} \ln 2 = 2 \cdot 2^e \ln 2 \leq 4 \cdot x \ln 2 = (4 \ln 2) \cdot x$$

This proves the lemma. ♣

Lemma: (*Chebyshev*) There are positive constants c, C so that

$$cx \leq \psi(x) \leq Cx$$

Proof: Consider

$$I = \int_0^1 x^n (1-x)^n dx$$

Multiplying out the $(1-x)^n$ and integrating term-by-term, no term has a denominator larger than $2n+1$, so if we multiply out by the least common multiple of $1, 2, 3, \dots, 2n+1$ the result is an integer:

$$I \times \text{lcm}(1, 2, 3, \dots, 2n, 2n+1) \in \mathbf{Z}$$

Thus,

$$1 \leq I \times \text{lcm}(1, 2, 3, \dots, 2n, 2n+1)$$

or

$$\frac{1}{I} \leq \text{lcm}(1, 2, 3, \dots, 2n, 2n+1)$$

On the other hand, the maximum of $x(1-x)$ on the interval $[0, 1]$ is $1/4$, so the integrand is at most $(1/4)^n$, and

$$I \leq \left(\frac{1}{4}\right)^n$$

which can be rearranged to

$$4^n \leq \frac{1}{I}$$

Thus, putting these inequalities together, we have

$$4^n \leq \text{lcm}(1, 2, 3, \dots, 2n, 2n+1)$$

Taking logarithms,

$$(\ln 4) \cdot n \leq \ln \text{lcm}(1, 2, 3, \dots, 2n+1)$$

Now we are happy, because of the following essentially elementary observation (which of course was the real reason that Chebyshev introduced ψ in the first place):

Lemma:

$$\psi(n) = \ln \text{lcm}(1, 2, 3, \dots, 2n+1)$$

(Proof left to the reader: it's not too hard!)

Finally we can return to the counting function $\pi(x)$ rather than the auxiliary functions θ and ψ . We have a **Riemann-Stieltjes integral**

$$\pi(x) = \int_{3/2}^x \frac{1}{\ln t} d\theta(t)$$

Integrating by parts, this gives

$$\pi(x) = \frac{\theta(x)}{\ln x} + \int_{3/2}^x \frac{\theta(t)}{t \ln^2 t} dt$$

Using the fact that $\theta(x) = O(x)$, this gives

$$\pi(x) = \frac{\theta(x)}{\ln x} + \int_{3/2}^x \frac{O(t)}{t \ln^2 t} dt = \frac{\theta(x)}{\ln x} + O\left(\frac{x}{\ln^2 x}\right)$$

Since we know by now that

$$cx \leq \theta(x) \leq Cx$$

for some positive constants c, C ,

$$\frac{cx}{\ln x} \leq \theta(x) \leq \frac{Cx}{\ln x}$$

This finishes the proof of the theorem. ♣

7.4 Sharpest known asymptotics

The best known assertion about asymptotic distribution of primes is somewhat sharper than the simple statement of the Prime Number Theorem, since it gives an *error term*. This result comes from work of I. Vinogradov and Korobov, but was finished in all details by A. Walfisz and H.-E. Rickert. See A. Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1963. A reasonable exposition in English of this and related results is in A. A. Karatsuba, *The distribution of prime numbers*, Russian Math. Surveys 45 (1990), pp. 99-171.

The **logarithmic integral** is defined to be

$$\operatorname{li}(x) = \int_2^x \frac{1}{\ln t} dt \quad \left(\sim \frac{x}{\ln x} \right)$$

The sharpest assertion proven concerning the distribution of primes (in 1997) seems to be: *there exists a positive constant c so that*

$$\pi(x) = \operatorname{li}(x) + O\left(\frac{x}{e^{c(\ln x)^{3/5}} (\ln \ln x)^{-1/5}}\right)$$

To simplify a little for clarity, we can weaken this statement to assert

$$\pi(x) = \frac{x}{\ln x} + O\left(\frac{x}{\ln^2 x}\right)$$

Since $\operatorname{li}(x)$ is monotone increasing, it has an inverse function. Write

$$\operatorname{li}^{-1}(x)$$

for the *inverse function* (not for $1/\operatorname{li}(x)$). Then the n^{th} prime p_n is estimated by

$$p_n = \operatorname{li}^{-1}(n) + O\left(\frac{n}{e^{(\ln n)^{3/5}} (\ln \ln n)^{-1/5}}\right) (\sim n \ln n)$$

7.5 The Riemann Hypothesis

Even though the Prime Number Theorem was not proven until 1896, already by 1858 B. Riemann had seen the connection between error terms in the distribution of primes and the subtle behavior of a special function, the **zeta function** defined below.

For a complex number s with real part > 1 , the series

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$$

is absolutely convergent, and defines a function of s . This is the **zeta function**, often called **Riemann's** because G. Riemann (about 1858) was the first to see that analytical properties of $\zeta(s)$ are intimately related to delicate details concerning the distribution of primes. Other people (for example, L. Euler) had seen that there were general connections. Already Euler had observed the **Euler product expansion**: for complex s with real part > 1

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p^s}}$$

To give this function meaning when the real part of s is less than or equal to 1 is already an issue, but this was resolved more than 140 years ago by Riemann, if not already by Euler.

For a real number r in the range $\frac{1}{2} < r < 1$, let PNT_r be the statement

$$\pi(x) = \frac{x}{\ln x} + O(x^{r+\varepsilon}) \quad \text{for all } \varepsilon > 0$$

It is important to realize that there is presently no proof that any such assertion is true: the **error term** in this assertion is asymptotically smaller than any error term that anyone has proven to hold. (See above.)

On the other hand, again for a real number r in the range $\frac{1}{2} < r < 1$, let RH_r be the statement

$$\zeta(s) \neq 0 \quad \text{when the real part of } s \text{ is } > r$$

No one has been able to prove any such statement for any $r < 1$. At the same time, it is known that there are *infinitely-many* complex numbers ρ with real part $\frac{1}{2}$ so that $\zeta(\rho) = 0$.

Theorem: (*sketched by Riemann*) For each $\frac{1}{2} < r < 1$, the assertion PNT_r is **equivalent** to RH_r .

In particular, the **Riemann Hypothesis** is that $\zeta(s) \neq 0$ for complex s with real part $> \frac{1}{2}$.

Thus, the *best possible error term* in the description of the asymptotic distribution of primes would be obtained if the Riemann Hypothesis were known to be true. But essentially nothing is known in this direction, although the accumulation of numerical evidence strongly supports the truth of the Riemann Hypothesis. *If* the Riemann Hypothesis is true, in fact (as H. von Koch has proven)

$$\begin{aligned} \pi(x) &= \text{li}(x) + O(\sqrt{x} \ln x) \\ n^{\text{th}} \text{ prime} &= \text{li}^{-1}(n) + O(\sqrt{n} (\ln n)^{5/2}) \end{aligned}$$

Then there is the **Extended Riemann Hypothesis** which is similar assertion about the zeros of a wider class of functions than just the zeta function. And the **Generalized Riemann Hypothesis** is a comparable assertion about the zeros of a yet wider class. All these hypotheses, if true, would give the best possible error estimates on the distribution of primes and generalizations of primes. Unfortunately, essentially nothing is known about these things, apart from numerical evidence in favor of all of them.

8. Sun Ze's Theorem

Now we start developing some standard classical number theory, on the way to understanding (for example) the structure of \mathbf{Z}/n , and this differences in this structure depending upon whether or not n is prime.

- Sun Ze's theorem
 - Special systems of linear congruences
 - Congruences with composite moduli
 - Hensel's lemma for prime-power moduli
-

8.1 Sun Ze's Theorem

The result of this section is sometimes known as the **Chinese Remainder Theorem**, mainly because the earliest results (including and following Sun Ze's) were obtained in China. Sun Ze's result was obtained before 450, and the statement below was obtained by Chin Chiu Shao about 1250. Such results, with virtually the same proofs, apply to much more general "numbers" than the integers \mathbf{Z} .

Let m_1, \dots, m_n be non-zero integers such that for any pair of indices i, j with $i \neq j$ the integers m_i and m_j are relatively prime. We say that the integers m_i are **mutually relatively prime**. Let

$$\mathbf{Z}/m_1 \times \mathbf{Z}/m_2 \times \dots \times \mathbf{Z}/m_n$$

denote (as usual) the collection of ordered n -tuples with the i^{th} item lying in \mathbf{Z}/m_i . Define a map

$$f : \mathbf{Z}/(m_1 \dots m_n) \rightarrow \mathbf{Z}/m_1 \times \mathbf{Z}/m_2 \times \dots \times \mathbf{Z}/m_n$$

by

$$f(x \text{ mod } (m_1 \dots m_n)) = (x \text{ mod } m_1, x \text{ mod } m_2, \dots, x \text{ mod } m_n)$$

Theorem: (*Sun-Ze*) For m_1, \dots, m_n mutually relatively prime, this map

$$f : \mathbf{Z}/(m_1 \dots m_n) \rightarrow \mathbf{Z}/m_1 \times \mathbf{Z}/m_2 \times \dots \times \mathbf{Z}/m_n$$

is a *bijection*.

Proof: First, we consider the case that there are just two different relatively prime moduli m, n , and to show that the corresponding map

$$f : \mathbf{Z}/mn \rightarrow \mathbf{Z}/m \times \mathbf{Z}/n$$

given by

$$f(x \text{ mod } mn) = (x \text{ mod } m, x \text{ mod } n)$$

is a bijection. First, we prove *injectivity*: if $f(x) = f(y)$, then $x \equiv y \pmod{m}$ and $x \equiv y \pmod{n}$. That is, $m|x - y$ and $n|x - y$. Since m, n are relatively prime (!), this implies that $mn|x - y$, so $x \equiv y \pmod{mn}$.

At this point, since \mathbf{Z}/mn and $\mathbf{Z}/m \times \mathbf{Z}/n$ are *finite* sets with the same number of elements (namely mn), any injective map must be surjective. So we could stop now and say that we know that f is surjective (hence bijective).

But it is worthwhile to understand the surjectivity more tangibly, to see once more where the relative prime-ness of m, n enters. Since m, n are relatively prime, there are integers s, t so that

$$sm + tn = 1$$

(We can find these s, t via the Euclidean Algorithm if we want, but that's not the point just now.) Then we claim that given integers a and b ,

$$f((b(sm) + a(tn)) \text{ mod } mn) = (a \text{ mod } m, b \text{ mod } n)$$

Indeed,

$$b(sm) + a(tn) \equiv b(sm) + a(1 - sm) \equiv a \pmod{m}$$

and similarly

$$b(sm) + a(tn) \equiv b(1 - tn) + a(tn) \equiv b \pmod{n}$$

This proves the surjectivity, and thus the bijectivity of the function f in the case of just two moduli.

Now consider an arbitrary number of (mutually relatively prime) moduli m_1, \dots, m_n . We'll do induction on the number n of moduli involved. The case $n = 2$ was just treated, and if $n = 1$ there is nothing to prove. So take $n > 2$. By induction on n , the map

$$f_o : \mathbf{Z}/m_2 \dots m_n \rightarrow \mathbf{Z}/m_2 \times \mathbf{Z}/m_3 \times \dots \times \mathbf{Z}/m_n$$

defined by

$$f_o(x \text{ mod } m_2 \dots m_n) = (x \text{ mod } m_2, x \text{ mod } m_3, \dots, x \text{ mod } m_n)$$

is a bijection. Thus, the map

$$f_1 : \mathbf{Z}/m_1 \times \mathbf{Z}/m_2 \dots m_n \rightarrow \mathbf{Z}/m_1 \times \mathbf{Z}/m_2 \times \mathbf{Z}/m_3 \times \dots \times \mathbf{Z}/m_n$$

defined by

$$f_1(x \text{ mod } m_1, x \text{ mod } m_2 \dots m_n) = (x \text{ mod } m_1, x \text{ mod } m_2, x \text{ mod } m_3, \dots, x \text{ mod } m_n)$$

is a bijection.

At the same time, invoking unique factorization (!), m_1 and the product $m_2 m_3 \dots m_n$ are relatively prime, so the case $n = 2$ gives the bijectivity of the map

$$f_2 : \mathbf{Z}/m_1(m_2 \dots m_n) \rightarrow \mathbf{Z}/m_1 \times \mathbf{Z}/m_2 \dots m_n$$

defined by

$$f_2(x \text{ mod } m_1(m_2 \dots m_n)) = (x \text{ mod } m_1, x \text{ mod } m_2 \dots m_n)$$

Therefore, the composite map

$$f = f_2 \circ f_1$$

is also a bijection. ♣

8.2 Special systems of linear congruences

Now we paraphrase the theorem above in terms of solving several congruences simultaneously. There are some similarities to the more elementary discussion of systems of linear *equations*, but there are critical differences, as well.

To start with, let's take the smallest non-trivial systems, of the form

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

where m, n are *relatively prime*, a, b are arbitrary integers, and we are to find all integers x which satisfy this system.

Notice that there are *two* congruences but just one *unknown*, which in the case of *equations* would probably lead to non-solvability immediately. But systems of congruences behave slightly differently. Our only concession is: **We'll only consider the case that the moduli m and n are relatively prime, that is, that $\gcd(m, n) = 1$.**

Using the Euclidean algorithm again, there are integers s, t so that

$$sm + tn = 1$$

since we supposed that $\gcd(m, n) = 1$. And this can be rearranged to

$$tn = 1 - sm$$

for example. **Here comes the trick:** the claim is that **the single congruence**

$$x_o = a(tn) + b(sm) \pmod{mn}$$

is equivalent to (has the same set of solutions) as the *system* of congruences above.

Let's check: modulo m , we have

$$\begin{aligned} x_o &\equiv (a(tn) + b(sm)) \pmod{m} \equiv a(tn) + 0 \pmod{m} \\ &\equiv a(tn) \pmod{m} \equiv a(1 - sm) \pmod{m} \\ &\equiv a(1) \pmod{m} \equiv a \pmod{m} \end{aligned}$$

The discussion of the congruence modulo n is nearly identical, with roles reversed. Let's do it:

$$\begin{aligned} x_o &\equiv (a(tn) + b(sm)) \pmod{n} \equiv 0 + b(sm) \pmod{n} \\ &\equiv b(sm) \pmod{n} \equiv b(1 - tn) \pmod{n} \\ &\equiv b(1) \pmod{n} \equiv b \pmod{n} \end{aligned}$$

Thus, anything congruent to this x_o modulo mn is a solution to the system.

On the other hand, suppose x is a solution to the system, and let's prove that it is congruent to x_o modulo mn . Since $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, we have

$$x - x_o \equiv a - a \equiv 0 \pmod{m}$$

and

$$x - x_o \equiv b - b \equiv 0 \pmod{n}$$

That is, both m and n divide $x - x_o$. Since m and n are *relatively prime*, we can conclude that mn divides $x - x_o$, as desired.

Note the process of sticking the solutions together via the goofy formula above uses the Euclidean Algorithm in order to be computationally effective (rather than just theoretically *possible*).

For example, let's solve the system

$$\begin{cases} x \equiv 2 \pmod{11} \\ x \equiv 7 \pmod{13} \end{cases}$$

To 'glue' these congruences together, we execute the Euclidean Algorithm on 11 and 13, to find

$$6 \cdot 11 - 5 \cdot 13 = 1$$

Thus, using the goofy formula above, the single congruence

$$x \equiv 2(-5 \cdot 13) + 7(6 \cdot 11) \pmod{11 \cdot 13}$$

is equivalent to the given system. In particular, this gives the solution

$$x \equiv -2 \cdot 5 \cdot 13 + 7 \cdot 6 \cdot 11 \equiv 332 \pmod{11 \cdot 13}$$

Quite generally, consider a system

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ x \equiv b_3 \pmod{m_3} \\ \dots \\ x \equiv b_n \pmod{m_n} \end{cases}$$

We'll only consider the scenario that m_i and m_j are relatively prime (for $i \neq j$). We solve it in steps: first, just look at the subsystem

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$$

and use the method above to turn this into a single (equivalent!) congruence of the form

$$x \equiv c_2 \pmod{m_1 m_2}$$

Then look at the system

$$\begin{cases} x \equiv c_2 \pmod{m_1 m_2} \\ x \equiv b_3 \pmod{m_3} \end{cases}$$

and use the method above to combine these two congruences into a single equivalent one, say

$$x \equiv c_3 \pmod{m_1 m_2 m_3}$$

and so on.

Remark: Yes, this procedure is just a paraphrase of the proof of the previous section.

8.3 Congruences with composite moduli

In general, to solve a congruence such as $x^2 \equiv b \pmod{m}$ with *composite* modulus $m = m_1 m_2$ (with m_1 and m_2 relatively prime), it is faster to solve the congruence modulo m_1 and m_2 *separately* and use Sun Ze's theorem to glue the solutions together into a solution modulo m , rather than trying to solve modulo m . This is especially true if the prime factorization of m is known.

For example, let's try to solve

$$x^2 \equiv -1 \pmod{13 \cdot 17 \cdot 29}$$

by hand (so that a brute force search is unreasonable, since we would not want to search through any significant fraction of $13 \cdot 17 \cdot 29 = 6409$ possibilities by hand!). We observe that Sun Ze's theorem asserts that the collection of integers x modulo 6409 satisfying $x^2 \equiv -1 \pmod{6409}$ is in bijection with the set of triples (x_1, x_2, x_3) where $x_1 \in \mathbf{Z}/13$, $x_2 \in \mathbf{Z}/17$, and $x_3 \in \mathbf{Z}/29$ and

$$x_1^2 \equiv -1 \pmod{13} \quad x_2^2 \equiv -1 \pmod{17} \quad x_3^2 \equiv -1 \pmod{29}$$

The bijection is

$$x \pmod{6409} \rightarrow (x \pmod{13}, x \pmod{17}, x \pmod{29})$$

Further, the discussion above tells how to go in the other direction, that is, to get back from $\mathbf{Z}/13 \times \mathbf{Z}/17 \times \mathbf{Z}/29$.

In this example, since the numbers 13, 17, 29 are not terribly large, a brute force search for square roots of -1 modulo 13, 17, and 29 won't take very long. Let's describe such a search in the case of modulus 29. First, $-1 = 28$ modulo 29, but 28 is not a square. Next, add 29 to 28: 57 is not a square. Add 29 to 57: 86 is not a square. Add 29 to 86: 115 is not a square. Add 29 to 115: $144 = 12^2$. Thus, ± 12 are square roots of -1 modulo 29. Similarly, we find that ± 5 are square roots of -1 modulo 13, and ± 4 are square roots of -1 modulo 17.

To use Sun Ze's theorem to get a solution modulo $6409 = 13 \cdot 17 \cdot 29$ from this, we first need integers s, t so that $s \cdot 13 + t \cdot 17 = 1$. The theoretical results about *gcd's* guarantee that there are such s, t , and Euclid's algorithm finds them:

$$\begin{aligned} 17 - 1 \cdot 13 &= 4 \\ 13 - 3 \cdot 4 &= 1 \end{aligned}$$

Going backwards:

$$\begin{aligned} 1 &= 13 - 3 \cdot 4 \\ &= 13 - 3 \cdot (17 - 1 \cdot 13) \\ &= 4 \cdot 13 - 3 \cdot 17 \end{aligned}$$

Therefore, from the square root 5 of -1 modulo 13 and square root 4 of -1 modulo 17 we get a square root of -1 modulo $13 \cdot 17$:

$$4(4 \cdot 13) - 5(3 \cdot 17) = -47 \pmod{13 \cdot 17}$$

Proceeding further, now we need integers s, t so that

$$s \cdot (13 \cdot 17) + t \cdot 29 = 1$$

Apply Euclid's algorithm, noting that $13 \cdot 17 = 221$:

$$\begin{aligned} 221 - 7 \cdot 29 &= 18 \\ 29 - 1 \cdot 18 &= 11 \\ 18 - 1 \cdot 11 &= 7 \\ 11 - 1 \cdot 7 &= 4 \\ 7 - 1 \cdot 4 &= 3 \\ 4 - 1 \cdot 3 &= 1 \end{aligned}$$

Going back, we get

$$\begin{aligned}
 1 &= 4 - 1 \cdot 3 \\
 &= 4 - 1 \cdot (7 - 4) \\
 &= 2 \cdot 4 - 1 \cdot 7 \\
 &= 2 \cdot (11 - 7) - 7 \\
 &= 2 \cdot 11 - 3 \cdot 7 \\
 &= 2 \cdot 11 - 3(18 - 11) \\
 &= 5 \cdot 11 - 3 \cdot 18 \\
 &= 5(29 - 18) - 3 \cdot 18 \\
 &= 5 \cdot 29 - 8 \cdot 18 \\
 &= 5 \cdot 29 - 8(221 - 7 \cdot 29) \\
 &= 61 \cdot 29 - 8 \cdot 221
 \end{aligned}$$

Therefore, from the square root -47 of -1 modulo $221 = 13 \cdot 17$ and the square root 12 of -1 modulo 29 we get the square root

$$12(-8 \cdot 221) + (-47)(61 \cdot 29) = -104359 = 4594 \pmod{6409}$$

Further, the most tedious part of the above procedure doesn't need to be repeated to find the other 7 (!) square roots of -1 modulo $13 \cdot 17 \cdot 29$, since we already have the numbers “s,t” in our possession.

8.4 Hensel's Lemma for prime-power moduli

In many cases, solving a polynomial equation $f(x) \equiv 0 \pmod{p}$ modulo a prime p suffices to assure that there are solutions modulo p^n for powers p^n of p , and also to find such solutions efficiently. And, funnily enough, the procedure to do so is exactly parallel to Newton's method for numerical approximation to roots, from calculus. In particular, we will use a purely algebraic form of Taylor expansions to prove the result.

First we'll do a numerical example to illustrate the idea of the process to which Hensel's Lemma refers. Suppose we want to find x so that $x^2 \equiv 2 \pmod{7^3}$. Noting that a solution mod 7^3 certainly must give a solution mod 7 , we'll start by finding a solution mod 7 . This is much easier, since there are only 7 things in $\mathbf{Z}/7$, and by a very quick trial and error hunt we see that $(\pm 3)^2 = 9 = 2 \pmod{7}$.

Now comes the trick: being optimists, we imagine that we can simply *adjust* the solution $3 \pmod{7}$ to obtain a solution mod 7^2 by adding (or subtracting) some multiple of 7 to it. That is, we imagine that for some $y \in \mathbf{Z}$

$$(3 + 7 \cdot y)^2 \equiv 2 \pmod{49}$$

Multiplying out, we have

$$9 + 21y + 49y^2 \equiv 2 \pmod{49}$$

Happily, the y^2 term disappears (modulo 49), because its coefficient is divisible by 49. Rearranging, this is

$$7 + 42y \equiv 0 \pmod{49}$$

Dividing through by 7 gives

$$1 + 6y \equiv 0 \pmod{7}$$

Since the coefficient (namely, 6) of y is invertible modulo 7, with inverse 6, we find a solution $y = (6^{-1})(-1) = 6 \cdot (-1) = 1 \pmod{7}$. Thus,

$$3 + 7 \cdot 1 = 10$$

is a square root of 2 modulo 7^2 .

Continuing in our optimism: Now we hope that we can *adjust* the solution $10 \pmod{7^2}$ by adding some multiple of 7^2 to it in order to get a solution $\pmod{7^3}$. That is, we hope to find y so that

$$(10 + 7^2y)^2 \equiv 2 \pmod{7^3}$$

Multiplying out and simplifying, this is

$$294y \equiv -98 \pmod{7^3}$$

Dividing through by 7^2 gives

$$6y \equiv -2 \pmod{7}$$

Again, the inverse of $6 \pmod{7}$ is just 6 again, so this is

$$y \equiv 6(-2) \equiv 2 \pmod{7}$$

Therefore,

$$10 + 7^2 \cdot 2 = 108$$

satisfies

$$108^2 \equiv 2 \pmod{7^3}$$

This was considerably faster than brute-force hunting for a square root of $2 \pmod{7^3}$ directly.

To prepare for a more general assertion of Hensel's Lemma, we need to give a purely algebraic description of the **derivative** of a polynomial. That is, we don't want the definition to require taking any limits. Let

$$f(x) = c_n x^n + \dots + c_0$$

with the coefficients in Z . Simply *define* another polynomial f' by

$$f'(x) = nc_n x^{n-1} + (n-1)c_{n-1} x^{n-2} + \dots + 2c_2 x + c_1 + 0$$

Remark: Of course, we have *defined* this derivative by the formula that we know is "correct" *if* it were defined as a limit.

Proposition: Using the purely algebraic definition of derivative, for polynomials f, g with coefficients in Z , and for $r \in Z$, we have

$$\begin{aligned}(rf)' &= rf' && \text{(constant-multiple rule)} \\ (f+g)' &= f' + g' && \text{(sum rule)} \\ (fg)' &= f'g + fg' && \text{(product rule)} \\ f \circ g &= f' \circ g \cdot g && \text{(chain rule)}\end{aligned}$$

Proof: We know from calculus that these assertions hold, even though we didn't mention limits here. ♣

Theorem: (*Hensel's Lemma*) Let f be a polynomial with coefficients in \mathbf{Z} . Let p be a prime number, and suppose that $x_n \in \mathbf{Z}$ satisfies

$$f(x_n) \equiv 0 \pmod{p^n}$$

with $n > 0$. Suppose that $f'(x_n) \not\equiv 0 \pmod{p}$. Let $f'(x_1)^{-1}$ be an integer which is a multiplicative inverse to $f'(x_1)$ modulo p . Then

$$x_{n+1} = x_n - f(x_n) f'(x_1)^{-1}$$

satisfies

$$f(x_{n+1}) \equiv 0 \pmod{p^{n+1}}$$

Further, from this construction,

$$x_{n+1} = x_n \pmod{p^n}$$

In particular, for every index,

$$x_n = x_1 \pmod{p}$$

Remark: Note that the quantity $f'(x_1)^{-1} \pmod{p}$ does not need to be recomputed each cycle of the iteration, but only once at the beginning.

Proof: First, let's check that if f has integer coefficients, then for every positive integer k the quotient $f^{(k)}/k!$ has integer coefficients, where $f^{(k)}$ is the k^{th} derivative of f . To prove this it suffices to look at $f(x) = x^n$, since every polynomial with integer coefficients is a sum of multiples of such things. In this case, $f^{(k)}/k! = \binom{n}{k} x^{n-k}$. Since $\binom{n}{k}$ appears as a coefficient in $(x+1)^n$, which has integer coefficients (!), this proves what we wanted.

Now we can almost prove the theorem. Let $y = -f(x_n) f'(x_n)^{-1} \pmod{p^{n+1}}$. Note that this expression uses $f'(x_n)^{-1} \pmod{p^{n+1}}$ instead of $f'(x_1)^{-1} \pmod{p}$. We'll have to come back at the end and take care of this adjustment.

We have $y \equiv 0 \pmod{p^n}$. Since f is a polynomial, a Taylor expansion for it about *any* point is finite, and converges to f . Thus,

$$f(x_n + y) = f(x_n) + \frac{f'(x_n)}{1!}y + \frac{f''(x_n)}{2!}y^2 + \frac{f^{(3)}(x_n)}{3!}y^3 + \dots$$

(The sum is finite!) Each $f^{(i)}(x_n)/i!$ is an integer, and p^{2n} divides y^2, y^3, y^4, \dots , so

$$p^{2n} \text{ divides } \frac{f''(x_n)}{2!}y^2 + \frac{f^{(3)}(x_n)}{3!}y^3 + \dots$$

And

$$f(x_n) + \frac{f'(x_n)}{1!}y = f(x_n) + \frac{f'(x_n)}{1!}(-f(x_n) f'(x_n)^{-1})$$

Since $f'(x_n)^{-1}$ is a multiplicative inverse of $f'(x_n)$ modulo p , there is an integer t so that

$$f'(x_n) \cdot f'(x_n)^{-1} = 1 + tp$$

Then

$$f(x_n) + \frac{f'(x_n)}{1!}y = f(x_n) + \frac{f'(x_n)}{1!}(-f(x_n) f'(x_n)^{-1}) = f(x_n) - f(x_n)(1 + tp) = f(x_n) \cdot tp$$

Since $f(x_n) \equiv 0 \pmod{p^n}$, and we have picked up one further factor of p , this is 0 modulo p^{n+1} , as claimed.

Further, regarding the last assertions of the theorem, note the quantity $f(x_n)/f'(x_n)$ by which we adjust x_n to get x_{n+1} is a multiple of p^n .

Finally, we need to check that

$$f(x_n)f'(x_n)^{-1} = f(x_n)f'(x_1)^{-1} \pmod{p^{n+1}}$$

where $f'(x_1)^{-1}$ is just an inverse mod p , not mod p^{n+1} . Since $x_n = x_1 \pmod{p}$, and since f' has integer coefficients, it is not so hard to check that

$$f'(x_n) = f'(x_1) \pmod{p}$$

Therefore,

$$f'(x_n)^{-1} = f'(x_1)^{-1} \pmod{p}$$

Further, by hypothesis p^n divides $f(x_n)$, so, multiplying through by $f(x_n)$ gives

$$f(x_n)f'(x_n)^{-1} = f(x_n)f'(x_1)^{-1} \pmod{p \cdot p^n}$$

This verifies that we don't need to compute $f'(x_n)^{-1} \pmod{p^{n+1}}$, but just the single quantity $f'(x_1)^{-1}$. ♣

Remark: We could give purely algebraic proofs of the differentiation formulas and the representability of polynomials by their Taylor expansions, but this can be done later in greater generality anyway, so we'll be content with the calculus-based argument here.

#8.68 Find an integer x so that $x \equiv 3 \pmod{5}$ and $x \equiv 4 \pmod{7}$.

#8.69 Find an integer x so that $3x \equiv 2 \pmod{5}$ and $4x \equiv 5 \pmod{7}$.

#8.70 Find four integers x which are distinct modulo $5 \cdot 7$ and so that $x^2 \equiv 1 \pmod{5}$ and $x^2 \equiv 1 \pmod{7}$. That is, find 4 *different* square roots of 1 modulo 35.

#8.71 Find four different square roots of 2 modulo $7 \cdot 23$.

#8.72 Explain why there are 8 different square roots of 1 modulo $3 \cdot 5 \cdot 7 = 105$.

#8.73 Find $\sqrt{2} \pmod{7^5}$ via Hensel's Lemma.

#8.74 Find $\sqrt{-1} \pmod{5^6}$ via Hensel's Lemma.

#8.75 (*) Discuss the failure of the *Quadratic Formula* to solve the equation $x^2 + x + 1 \equiv 0 \pmod{2}$.

9. Good algorithm for exponentiation

- Fast exponentiation
-

9.1 Fast exponentiation

The most naive version of exponentiation, in which to compute x^n one computes x^2 , then $x^3 = x \cdot x^2$, then $x^4 = x \cdot x^3$, ..., $x^n = x \cdot x^{n-1}$, is very inefficient. Here we note a very simple but much faster improvement upon this, which has been known for at least 3000 years. This improvement is especially relevant for exponentiation modulo m .

The idea is that to compute x^e we express e as a *binary* integer

$$e = e_0 + e_1 \cdot 2^1 + e_2 \cdot 2^2 + \dots + e_n \cdot 2^n$$

with each e_i equal to 0 or 1, and compute power-of-two powers of x **by squaring**:

$$\begin{aligned}x^2 &= x \cdot x \\x^4 &= (x^2)^2 \\x^8 &= (x^4)^2 \\x^{2^4} &= (x^8)^2 \\x^{2^5} &= (x^{2^4})^2 \\&\dots\end{aligned}$$

Then

$$x^e = x^{e_0} (x^2)^{e_1} (x^4)^{e_2} (x^8)^{e_3} (x^{2^4})^{e_4} \dots (x^{2^n})^{e_n}$$

Again, the e_i 's are just 0 or 1, so in fact this notation is clumsy: we *omit* the factor x^{2^k} if $e_k = 0$ and *include* the factor x^{2^k} if $e_k = 1$.

A fairly good way of implementing this is the following. To compute x^e , we will keep track of a triple (X, E, Y) which initially is $(X, E, Y) = (x, e, 1)$. At each step of the algorithm:

- If E is odd then replace Y by $X \times Y$ and replace E by $E - 1$
- If E is even then replace X by $X \times X$ and replace E by $E/2$. When $E = 0$ the value of Y at that time is x^e .

This algorithm takes at most $2 \log_2 E$ steps (although of course the numbers involved grow considerably!)

For our purposes, this pretty fast exponentiation algorithm is of special interest when combined with reduction modulo m : the rewritten algorithm is: to compute $x^e \% m$, we will keep track of a triple (X, E, Y) which initially is $(X, E, Y) = (x, e, 1)$. At each step of the algorithm:

- If E is odd then replace Y by $X \times Y \% m$ and replace E by $E - 1$
- If E is even then replace X by $X \times X \% m$ and replace E by $E/2$. When $E = 0$ the value of Y at that time is $x^e \% m$.

Again, this algorithm takes at most $2 \log_2 E$ steps. When the exponentiation is done modulo m , the numbers involved stay below m^2 , as well.

Note that in the fast exponentiation modulo m , no number larger than m^2 will arise. Thus, for example, to compute something like

$$2^{1000} \% 1000001$$

would require no more than $2 \log_2 1000 \approx 2 \cdot 10 = 20$ multiplications of 6-digit numbers. Generally, we have

Proposition: The above algorithm for evaluation of $x^e \% m$ uses $O(\log e \log^2 n)$ bit operations.

For example, let's directly evaluate $2^{1000} \bmod 89$. Setting this up as indicated just above, we have

'X'	'E'	'output'	
2	1000	1	initial state
4	500	1	'E' was even: square 'X' mod 89
16	250	1	'E' was even: square 'X' mod 89
78	125	1	'E' was even: square 'X' mod 89
78	124	78	'E' was odd: multiply 'out' by 'X' mod 89
32	62	78	'E' was even: square 'X' mod 89
45	31	78	'E' was even: square 'X' mod 89
45	30	39	'E' was odd: multiply 'out' by 'X' mod 89
67	15	39	'E' was even: square 'X' mod 89
67	14	32	'E' was odd: multiply 'out' by 'X' mod 89
39	7	32	'E' was even: square 'X' mod 89
39	6	2	'E' was odd: multiply 'out' by 'X' mod 89
8	3	2	'E' was even: square 'X' mod 89
8	2	16	'E' was odd: multiply 'out' by 'X' mod 89
64	1	16	'E' was even: square 'X' mod 89
64	0	45	'E' was odd: multiply 'out' by 'X' mod 89

We conclude that

$$2^{1000} \% 89 = 45$$

#9.76 Estimate the number of steps necessary to compute 2^{100} by the fast exponentiation algorithm.

#9.77 Compute $2^{33} \bmod 19$.

#9.78 Compute $2^{129} \bmod 19$.

#9.79 Compute $2^{127} \bmod 19$.

10. Fermat's Little Theorem

More than 350 years ago Pierre de Fermat made many astute observations regarding prime numbers, factorization into primes, and related aspects of number theory (not to mention other parts of mathematics and science as well.) About 300 years ago, Leonhard Euler systematically continued Fermat's work. Most of these things were prototypes for "modern" mathematical ideas, and at the same time remain very much relevant to contemporary number theory and its applications.

- Fermat's Little Theorem
- Factoring $b^n - 1$
- Examples: factoring Mersenne numbers
- Examples: factoring $3^n - 1$
- A formula for square roots mod p
- A formula for n^{th} roots mod p

10.1 Fermat's Little Theorem

This little result is over 350 years old. It is basic in elementary number theory itself, and is the origin of the first *probabilistic* primality test. It is possible to prove Fermat's Little Theorem with very minimal prerequisites, as we'll do now.

Theorem: Let p be a prime number. Then for any integer x

$$x^p \equiv x \pmod{p}$$

Proof: We will first prove that prime p divides the binomial coefficients

$$\binom{p}{i}$$

with $1 \leq i \leq p - 1$, keeping in mind that the "extreme" cases $i = 0$ and $i = p$ can't possibly also have this property, since

$$\binom{p}{0} = 1 \quad \binom{p}{p} = 1$$

Indeed, from its definition,

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

Certainly p divides the numerator. Since $0 < i < p$, the prime p divides none of the factors in the factorials in the denominator. By unique factorization into primes, this means that p does not divide the denominator at all.

From the Binomial Theorem,

$$(x + y)^p = \sum_{0 \leq i \leq p} \binom{p}{i} x^i y^{p-i}$$

In particular, since the coefficients of the left-hand side are integers the same must be true of the right-hand side. Thus, all the binomial coefficients are *integers*. (We did not use the fact that p is prime to reach *this* conclusion.

Thus, the binomial coefficients with $0 < i < p$ are *integers* expressed as fractions whose numerators are divisible by p and whose denominators are *not* divisible by p . Thus, when all cancellation is done in the fraction, there must remain a factor of p in the numerator. This proves the desired fact about binomial coefficients.

Now we prove Fermat's Little Theorem (for *positive* x) by induction on x . First, certainly $1^p \equiv 1 \pmod{p}$. For the induction step, suppose that we already know for some particular x that

$$x^p \equiv x \pmod{p}$$

Then

$$(x + 1)^p = \sum_{0 \leq i \leq p} \binom{p}{i} x^i 1^{p-i} = x^p + \sum_{0 < i < p} \binom{p}{i} x^i + 1$$

All the coefficients in the sum in the middle of the last expression are divisible by p . Therefore,

$$(x + 1)^p \equiv x^p + 0 + 1 \equiv x + 1 \pmod{p}$$

since our induction hypothesis is that $x^p \equiv x \pmod{p}$. This proves the theorem for positive x .

To prove the theorem for $x < 0$ we use the fact that $-x$ is then *positive*. For $p = 2$ we can just treat the two cases $x \equiv 0 \pmod{2}$ and $x \equiv 1 \pmod{2}$ separately and directly. For $p > 2$ we use the fact that such a prime is *odd*. Thus,

$$x^p = -(-x)^p \equiv -(-x) \pmod{p} = x \pmod{p}$$

by using the result for positive integers. ♣

10.2 Factoring $b^n - 1$

Using Fermat's Little Theorem, we can follow in his footsteps and speed up certain *special* factorizations by a significant factor. First we prove a Lemma that looks too good to be true:

Lemma: Let $b > 1$. Then for any two positive integers m, n ,

$$\gcd(b^m - 1, b^n - 1) = b^{\gcd(m, n)} - 1$$

Remark: From elementary algebra we should remember the identity

$$x^N - 1 = (x - 1)(x^{N-1} + x^{N-2} + \dots + x^2 + x + 1)$$

for positive integers N . For a positive divisor d of n , letting $x = b^d$ and $N = n/d$, we obtain

$$b^n - 1 = (b^d)^N - 1 = (b^d - 1)((b^d)^{N-1} + (b^d)^{N-2} + \dots + (b^d)^2 + (b^d) + 1)$$

Thus, for simple reasons $b^d - 1$ divides $b^n - 1$ for $d|n$.

Proof: First, note that if $m = n$ then the assertion of the proposition is certainly true. The rest of the proof is by induction on the larger of m, n . We may suppose that $m \leq n$ (reversing the roles of m, n if necessary). In the case that $n = 1$, the assertion would be that the gcd of $b - 1$ and $b - 1$ is $b - 1$, which is certainly true. Now the induction step. We may suppose that $m < n$, since the $m = n$ case has been treated already. Note that

$$(b^n - 1) - b^{n-m}(b^m - 1) = b^{n-m} - 1$$

We claim that

$$\gcd(b^m - 1, b^n - 1) = \gcd(b^m - 1, b^{n-m} - 1)$$

On one hand, if $d|b^n - 1$ and $d|b^m - 1$, then $d|(b^n - 1) - b^{n-m}(b^m - 1)$, and then $d|b^{n-m} - 1$. Thus, any common divisor d of $b^n - 1$ and $b^m - 1$ also is a divisor of $b^{n-m} - 1$. On the other hand, from the rearranged expression

$$b^n - 1 = b^{n-m}(b^m - 1) + b^{n-m} - 1$$

any common divisor of $b^m - 1$ and $b^{n-m} - 1$ divides the right-hand side, so divides $b^n - 1$. This proves the claim.

Thus, invoking the induction hypothesis, we have

$$\gcd(b^m - 1, b^n - 1) = \gcd(b^m - 1, b^{n-m} - 1) = b^{\gcd(m, n-m)} - 1$$

So we should show that $\gcd(m, n) = \gcd(m, n - m)$: this follows the same standard idea as the proof of the last claim: On one hand, certainly if d is a common divisor of m and n , then $d|n - m$. On the other hand, using $n = m + (n - m)$, if d is a common divisor of m and $n - m$ then $d|n$ as well. ♣

Corollary: Fix a positive integer b . Let n be a positive integer. If a prime p divides $b^n - 1$, then either $p|b^d - 1$ for some divisor d of n with $d < n$, or $p \equiv 1 \pmod n$.

Proof: Suppose that p divides $b^n - 1$. By Fermat's Little Theorem, $b^{p-1} \equiv 1 \pmod p$, so p divides $b^{p-1} - 1$. Therefore, by the lemma, p divides $b^{\gcd(n, p-1)} - 1$. If $d = \gcd(n, p-1) < n$, then certainly $d < n$ is a positive divisor of n with $p|b^d - 1$. If $\gcd(n, p-1) = n$, then $n|p-1$, which is to say that $p \equiv 1 \pmod n$. ♣

Remark: The latter corollary shows that divisors of numbers of the form $b^n - 1$ are considerably restricted. Further, for *odd* primes p and *odd* n , since $\gcd(n, 2) = 1$, if $n|p-1$ then from $2|p-1$ we can conclude that $2n|p-1$, so $p \equiv 1 \pmod{2n}$.

10.3 Examples: factoring Mersenne numbers

The restriction on the possible prime factors of numbers of the form $b^n - 1$ noted above reduces by a significant factor the time to factor (by otherwise naive methods) Mersenne numbers $2^n - 1$.

Example: Factor $127 = 2^7 - 1$: Since 7 is prime, the corollary shows that the only possible prime factors p of this number must satisfy $p \equiv 1 \pmod{14}$. On the other hand, $\sqrt{127} < 12$, so we need only attempt division by primes under 12. But there aren't any such things that are also congruent to 1 modulo 14, so $2^7 - 1$ must be prime.

Remark: Even though we could easily test primality of 127 by hand anyway, it is pretty cute that we can also do it "by pure thought" (meaning *without computing very much*).

Example: Factor $255 = 2^8 - 1$: The composite exponent yields many factors: from $2^2 - 1 = 3$ we get 3, from $2^4 - 1 = 15 = 3 \cdot 5$ we get 5. Dividing, we have

$$255/(3 \cdot 5) = 17$$

which is prime. So $2^8 - 1 = 3 \cdot 5 \cdot 17$.

Example: Factor $511 = 2^9 - 1$: The composite exponent gives a factor $2^3 - 1 = 7$. Then $511/7 = 73$, which is prime. So $2^9 - 1 = 7 \cdot 73$.

Example: Factor $1023 = 2^{10} - 1$: First, since the exponent is *composite*, this Mersenne number is certainly composite. We note that the (positive) divisors of 10 less than 10 are 1, 2, 5, so we have divisors $3 = 2^2 - 1$ and $31 = 2^5 - 1$ of $2^{10} - 1$. The corollary then tells us that any *other* primes dividing $2^{10} - 1$ must be congruent to 1 modulo 10. First try 11: indeed

$$1023/11 = 93 = 3 \cdot 31$$

So

$$1023 = 3 \cdot 11 \cdot 31$$

Of course, since $2^{10} - 1$ has the small factor 3, already $1023/3 = 341$ is small-enough that we might not mind continuing its factorization by hand? Especially after being handed the factor of $31 = 2^5 - 1$, and computing $341/31 = 11$, there's nothing left to the imagination.

Example: Factor $2047 = 2^{11} - 1$: Now we don't have any "cheap" factors, since 11 is prime. If this number were to turn out to be prime, then it would be a **Mersenne prime**. The corollary above assures us that any prime p dividing 2047 must satisfy $p \equiv 1 \pmod{11}$. Since also p must be *odd*, as noted above we can in fact assert that such p satisfies $p \equiv 1 \pmod{22}$. So we attempt division of 2047 by $23 = 22 + 1$, and find that $2047/23 = 89$. (Since $89 < 100$, trial division by merely 2, 3, 5, 7 shows that 89 is prime.) So $2047 = 23 \cdot 89$.

Example: Factor $4095 = 2^{12} - 1$: The exponent is so composite that we have many easy prime factors arising from the factors $2^d - 1$ with $d < 12$ dividing 12. That is, we can first look at the prime factors of $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^4 - 1 = 15 = 3 \cdot 5$, and $2^6 - 1 = 63 = 3^2 \cdot 7$. Thus, 4095 is divisible by $3^2 \cdot 5 \cdot 7$. Dividing, we are left with

$$4095/(3^2 \cdot 5 \cdot 7) = 13$$

So the whole factorization is $4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$.

Example: Factor $8191 = 2^{13} - 1$. The exponent 13 is prime, so there are no obvious factors. If this number were to turn out to be prime, then it would be a **Mersenne prime**. Since $\sqrt{8191} \approx 90.5$, we need only do trial division by primes under 90. The corollary above says that we need only consider primes $p \equiv 1 \pmod{26}$. First, $26 + 1 = 27$ is not prime, so we need not attempt division by it. Second, $2 \cdot 26 + 1 = 53$ is prime, but $8191 \% 53 = 29$. Then $3 \cdot 26 + 1 = 79$ is prime, but $8191 \% 79 = 54$. So 8191 is prime.

Example: Factor $16383 = 2^{14} - 1$. We look at $2^2 - 1 = 3$ and $2^7 - 1 = 127$ first. We saw above that 127 is prime. So we can take out prime factors of 3 and 127, leaving

$$16383/(3 \cdot 127) = 43$$

which we recognize as being prime.

Example: Factor $32767 = 2^{15} - 1$: From $2^3 - 1 = 7$ and $2^5 - 1 = 31$ we find prime factors 7 and 31. Dividing out, we have

$$32767/(7 \cdot 31) = 151$$

We could attack this by hand, or invoke the corollary to restrict our attention to primes p with $p \equiv 1 \pmod{30}$ which are less than $\sqrt{151} < 13$. Since there aren't any such primes, we can conclude for *qualitative* reasons that 151 is prime. Therefore, the prime factorization is $2^{15} - 1 = 7 \cdot 31 \cdot 151$.

Example: Factor $65535 = 2^{16} - 1$: From $2^2 - 1 = 3$, $2^4 - 1 = 15 = 3 \cdot 5$, $2^8 - 1 = 255 = 3 \cdot 5 \cdot 17$ (from above), we obtain prime factors 3, 5, and 17. Dividing, we get

$$65535/(3 \cdot 5 \cdot 17) = 257$$

Now we invoke the corollary to restrict our attention to potential prime factors p with $p \equiv 1 \pmod{16}$. At the same time, $\sqrt{257} < 17$. This excludes all candidates, so 257 is prime, and the prime factorization is

$$2^{16} - 1 = 3 \cdot 5 \cdot 17 \cdot 257$$

Example: Factor $131071 = 2^{17} - 1$: Since 17 is prime, we only look for prime factors p with $p \equiv 1 \pmod{34}$, and also $p \leq \sqrt{131071} < 362.038$. First, $34 + 1 = 35$ is not prime. Next, $2 \cdot 34 + 1 = 69$ is divisible by 3, so is not prime. Next, $3 \cdot 34 + 1 = 103$ is prime, but $131071 \% 103 = 55$. Next, $4 \cdot 34 + 1 = 137$ is prime, but $131071 \% 137 = 99$. Next, $5 \cdot 34 + 1 = 171$, which is divisible by 3. Next, $6 \cdot 34 + 1 = 205$, visibly divisible by 5. Next, $7 \cdot 34 + 1 = 239$, which is prime (testing prime divisors 2, 3, 5, 7, 11, 13 all $\leq \sqrt{239} < 16$). But $131071 \% 239 = 99$. Next, $8 \cdot 34 + 1 = 273$, which is divisible by 3. Next, $9 \cdot 34 + 1 = 307$, which is prime (testing prime divisors $\leq \sqrt{307} < 18$). But $131071 \% 307 = 289$. Next, $19 \cdot 34 + 1 = 341$, which is divisible by 11. Since this is the last candidate prime below the bound 362, it must be that $131071 = 2^{17} - 1$ is prime.

Example: It turns out that $524287 = 2^{19} - 1$ is prime. To verify this in the most naive way, we would have to look for possible prime divisors $\leq \sqrt{524287} < 725$. If we did this in the *most* naive way it would require about $725/2 \approx 362$ trial divisions to verify the primality. But if we invoke the lemma and restrict our attention to primes p with $p \equiv 1 \pmod{38}$, we'll only need about $725/38 \approx 19$ trial divisions.

Example: Factor $8388607 = 2^{23} - 1$: By the corollary, we need only look at primes p with $p \equiv 1 \pmod{46}$. And, by luck 47 divides this number. Divide, to obtain $8388607/47 = 178481$. Anticipating (!?) that this is a prime, we note that we must attempt division by primes $\leq \sqrt{178481} < 422.5$. Looking only at these special primes, we have about $422/46 \approx 9$ trial divisions to do, rather than the $422/2 \approx 211$ in the most naive approach.

Example: Factor $536870911 = 2^{29} - 1$: Any possible prime factors p satisfy $p \equiv 1 \pmod{58}$, and if this number is not prime then it has such a factor $\leq \sqrt{536870911} \approx 23170$. Looking at 59, 117 (not prime), 175 (not prime), 233, ..., by luck it happens that 233 divides 536870911. Divide:

$$536870911/233 = 2304167$$

The latter is not divisible by 233. We know that if 2304167 is not prime then it has a prime divisor $\leq \sqrt{2304167} < 1518$. After 14 more trial divisions, we would find that the prime $19 \cdot 58 + 1 = 1103$ divides 2304167. Dividing, we have $2304167/1103 = 2089$. If 2089 were not prime, then it would have a prime factor $\leq \sqrt{2089} < 46$, but also $\equiv 1 \pmod{58}$. There aren't any such things, so 2089 is prime. Therefore,

$$536870911 = 233 \cdot 1103 \cdot 2089$$

10.4 Factoring $3^n - 1$

We continue with more examples using Fermat's observation about factors of special numbers of the form $b^n - 1$.

Every number $3^n - 1$ (for $n > 1$) has the obvious factor $3 - 1$, so is not prime. But this is a rather weak statement, since we might want the whole prime factorization, or at least be curious whether or not $(3^n - 1)/(3 - 1)$ is prime. Fermat's trick is helpful in investigating this, in the same way that it was helpful in looking at Mersenne numbers.

The trick we have in mind here asserts that if a prime p divides $b^n - 1$ then either $p|(b^d - 1)$ for some $d|n$ with $d < n$, or else $p \equiv 1 \pmod{n}$. And if case n is odd then $p \equiv 1 \pmod{2n}$. Thus, in rough terms, the number of primes p to attempt to divide into $b^n - 1$ is reduced by a factor of n or $2n$.

First, $3^2 - 1 = 8 = 2^3$.

Next, $(3^3 - 1)/2 = 26/2 = 13$. Fermat's trick indicates that a prime dividing $3^3 - 1$ and not dividing $3^1 - 1$ should be congruent to 1 mod $2 \cdot 3 = 6$, which is the case with 13.

Next, $3^4 - 1 = (3^2 - 1)(3^2 + 1)$. We factored $3^2 - 1$ above. The factor $3^2 + 1$ is still certainly divisible by 2, and then $(3^2 + 1)/2 = 5$, which is indeed a prime congruent to 1 modulo 4.

Next, $3^5 - 1 = 242$. Taking out the factor $3 - 1$ leaves 121. By Fermat's trick, any prime dividing this must be congruent to 1 modulo $2 \cdot 5 = 10$. Trying $10 + 1 = 11$, we see that in fact (as we really probably knew all along) $121 = 11^2$.

Next, $3^6 - 1 = (3^3 - 1)(3^3 + 1) = (3^3 - 1)(3 + 1)(3^2 - 3 + 1)$. We already understand all the factors except $3^2 - 3 + 1 = 7$. Indeed, this is a prime congruent to 1 modulo 6.

Next, $3^7 - 1 = 2186$. Taking out the factor of $3 - 1 = 2$ leaves 1093. By Fermat's trick, we know that any prime factor of this must be congruent to 1 mod $2 \cdot 7 = 14$. Since $14 + 1 = 15$ is not prime, the first prime we try to divide into 1093 is $2 \cdot 14 + 1 = 29$, and we find that $1093 \% 29 = 20$. Now $\sqrt{1093} \approx 33.06 < 34$, so we know in advance that we need not test potential divisors for 1093 larger than 33. But 29 is the only prime < 34 and congruent to 1 modulo 14, so we're done: 1093 is prime.

Next $3^8 - 1 = (3^4 - 1)(3^4 + 1)$. After taking the factor of $3 - 1 = 2$ out of $3^4 + 1$ we have $(3^4 + 1)/2 = 41$. Fermat's trick assures us that any prime not dividing $3^4 - 1 = 80 = 2^4 \cdot 5$ and dividing this will be congruent to 1 modulo 8. Since there are no primes congruent to 1 mod 8 and $\leq \sqrt{41} < 7$, it follows that 41 is prime. (Yes, we already knew that anyway.)

Next, $(3^9 - 1)/(3^3 - 1) = 3^6 + 3^3 + 1 = 757$. From Fermat, 757 must be divisible only by primes congruent to 1 modulo $2 \cdot 9 = 18$. Also, if 757 is not prime then it will have a prime divisor $\leq \sqrt{757} < 28$. The only prime in this range is $18 + 1 = 19$, but $757 \% 19 = 16$, so 757 is prime.

Next, $(3^{10} - 1)/(3^5 - 1) = 244$. Taking out the factor of 2^2 , this is 61. This has no prime factors dividing $3^2 - 1 = 8$ nor $(3^5 - 1)/2 = 11^2$, so any prime factors of it must be congruent to 1 modulo 10. There are no such primes $\leq \sqrt{61} < 8$, so 61 is prime. (Yes, we knew that already.)

Next $(3^{11} - 1)/2 = 88573$. Any prime dividing this must be congruent to 1 modulo 22. Attempting division by the first such, 23, gives a quotient of 3851 with no remainder. Trying again, $3851 \% 23 = 10$, so 23 does not divide 3851. If 3851 is not prime, it has a prime divisor $\leq \sqrt{3851} \approx 62.06 < 63$. The next candidate, $23 + 22 = 45$, is not prime. The next candidate is $45 + 22 = 67$, which is prime, but is too large already. Therefore, 3851 is prime.

It turns out that $(3^{13} - 1)/2 = 797161$ is prime, but even with Fermat's speed-up, this would still take about 35 trial divisions. This is plausible to do "by hand", certainly better than the over 400 trial divisions that the most naive primality test would require.

Skipping ahead a little, let's look at $3^{15} - 1$. The quotient $(3^{15} - 1)/(3^5 - 1) = 59293$ has prime factors either dividing $3^3 - 1 = 2 \cdot 13$ or congruent to 1 modulo $2 \cdot 15 = 30$. Trying 13, we get $59293/13 = 4561$. (And 13 does not divide 4561.) The only prime divisors of *this* are congruent to 1 modulo 30. Also, if 4561 is not prime it must have a factor $\leq \sqrt{4561} \approx 67.54 < 68$. Trying 31, we find $4561 \% 31 = 4$. Trying 61, we find $4561 \% 61 = 47$. Thus, 4561 is prime.

10.5 A formula for some square roots

In the case that a prime p satisfies $p \equiv 3 \pmod{4}$ we can also give a *formula* for the square root of a square modulo p prime. Since we have a good algorithm for exponentiation, this formula should be viewed as reasonably good for finding square roots. Note that it only applies if the prime modulus p is congruent to 3 modulo 4, and only if the given number *really is a square mod p* . (Otherwise, the formula can be evaluated, but the output is garbage.)

Theorem: Let p be a prime satisfying $p \equiv 3 \pmod{4}$. Then for an integer y which is a square-modulo- p ,

$$x = y^{(p+1)/4} \pmod{p}$$

is a square-root-mod- p of y . That is, $x^2 \equiv y \pmod{p}$.

Remark: Unfortunately, if y is *not* a square modulo p , the formula can be evaluated, but does *not* give a square root of y modulo p . Also, unfortunately, for $p \equiv 1 \pmod{4}$ there is no formula for square roots analogous to this.

Proof: First note that the expression $(p+1)/4$ is not an integer unless $p \equiv 3 \pmod{4}$. Suppose that $y = x^2$. Let's check that $z = y^{(p+1)/4}$ has the property that $z^2 = y \pmod{p}$. (Note that we do *not* assert that $z = x$!) Then

$$(y^{(p+1)/4})^2 = y^{(p+1)/2} = (x^2)^{(p+1)/2} = x^{p+1} = x^p x^1 = x \cdot x = y$$

where we get $x^p = x \pmod{p}$ from Fermat's Little Theorem. ♣

10.6 A formula for n^{th} roots mod p

Generalizing the square root case above, in certain circumstances we have a formula to find n^{th} roots modulo p .

A non-zero y modulo p is an n^{th} -**power** (or, in archaic terminology, n^{th} -**power residue**) modulo p if there is x so that $x^n \equiv y \pmod{p}$. (If there is no such x , then y is an n^{th} -**power non-residue**.)

Theorem: Let p be a prime. If n is relatively prime to $p-1$, then *every* y has an n^{th} root modulo p . In particular, letting r be a multiplicative inverse for n modulo $p-1$,

$$n^{\text{th}} \text{ root of } y \pmod{p} = y^r$$

Proof: We check that $(y^r)^n = y \pmod{p}$. For $p|y$, so that $y = 0 \pmod{p}$, this is easy. So now suppose that p does not divide y . Since $rn \equiv 1 \pmod{p-1}$ there is a positive integer ℓ so that $rn = 1 + \ell(p-1)$. Then

$$(y^r)^n = y^{rn} = y^{1+\ell(p-1)} = y \cdot (y^{p-1})^\ell = y \cdot 1^\ell = y$$

since Fermat's Little Theorem gives $y^{p-1} = 1 \pmod{p}$. ♣

Having treated the case that $\gcd(n, p-1) = n$, we will ignore the intermediate cases where $1 < \gcd(n, p-1) < n$ and treat the other extreme where $\gcd(n, p-1) = 1$: We have a computationally effective way to compute n^{th} roots modulo primes p with $n|(p-1)$ as long as $\gcd(n, \frac{p-1}{n}) = 1$:

Theorem: Let p be a prime so that $p \equiv 1 \pmod n$, but so that $\gcd(n, \frac{p-1}{n}) = 1$. Let r be a multiplicative inverse of n modulo $(p-1)/n$. If y is an n^{th} power then

$$n^{\text{th}} \text{ root of } y \text{ mod } p = y^r$$

Proof: The basic mechanism of the argument is the same as the previous proof, with a few complications. We check that $(y^r)^n = y \pmod p$. For $p|y$, so that $y = 0 \pmod p$, this is easy. So now suppose that p does not divide y . Since $rn \equiv 1 \pmod{(p-1)/n}$ there is a positive integer ℓ so that $rn = 1 + \ell(p-1)/n$. Also, since we are assuming that y has an n^{th} root, we can express y as $y = x^n \pmod p$. Then

$$(y^r)^n = ((x^n)^r)^n = x^{n \cdot rn} = x^{n \cdot (1 + \frac{\ell(p-1)}{n})} = x^n \cdot x^{\ell(p-1)} = x^n \cdot (x^{p-1})^\ell = x^n \cdot 1^\ell = x^n = y \pmod p$$

where we invoke Fermat's Little Theorem to know that $x^{p-1} = 1 \pmod p$. ♣

Remark: The formula in the latter theorem yields *garbage* if y is *not* an n^{th} power!

Remark: If $\gcd(n, \frac{p-1}{n}) > 1$ then computation of roots is more complicated.

Remark: The difference between the two formulas for the n^{th} roots, for the two cases in the two theorems just above is very important. Application of either one in the *other* situation yields garbage.

#10.80 Factor $5^n - 1$ into primes for $1 \leq n \leq 11$.

#10.81 Find a square root of 2 mod 103.

#10.82 Find 11^{th} roots of 2 and 3 modulo 101.

#10.83 Find 11^{th} roots of 141 and 162 modulo 199.

#10.84 Show that 2 is *not* an 11^{th} power mod 199.

11. Euler's Theorem, Primitive Roots, Exponents, Roots

The direct successor to Fermat, Leonhard Euler systematically continued Fermat's work in number theory and its applications.

Some of the the proofs in this section are incomplete, since they depend on (for example) the existence of primitive roots modulo primes, which we can only prove later. Nevertheless, these results illustrate the relevance of the later more abstract results.

- Euler's Theorem
 - Facts about primitive roots
 - Euler's criterion for n^{th} roots mod p
-

11.1 Euler's Theorem

Here we *state* Euler's Theorem generalizing Fermat's Little Theorem. An intelligent proof of Euler's Theorem is best given as a corollary of some basic *group theory*, so we postpone the proof till later.

For a positive integer n , the **Euler phi-function** $\varphi(n)$ is the number of integers b so that $0 < b < n$ and $\gcd(b, n) = 1$.

Theorem: (Euler) For x relatively prime to a positive integer n ,

$$x^{\varphi(n)} = 1 \pmod{n}$$

(*Proof later.*)

The special case that n is prime is just Fermat's Little Theorem, since for prime p we easily see that $\varphi(p) = p - 1$.

11.2 Facts about primitive roots

In this section we simply *explain* what a **primitive root** is supposed to be, and state what is true. The *existence* of primitive roots *modulo primes* will be used just below to prove the "hard half" of Euler's criteria for whether or not things have square roots (or n^{th} roots) modulo primes. The proofs of *existence* (and non-existence) of primitive roots require more preparation.

Let n be a positive integer. An integer g is a **primitive root modulo n** if the smallest positive integer ℓ so that $g^\ell = 1 \pmod{n}$ is $\varphi(n)$.

Note that Euler's theorem assures us that in any case for g relatively prime to n no exponent ℓ larger than $\varphi(n)$ is necessary.

For "most" integers n there is *not* primitive root modulo n . The precise statement about when there is or is not a primitive root modulo m is

Theorem: The only integers n for which there is a primitive root modulo n are those of the forms

- $n = p^e$ with an odd prime p , and $e \geq 1$
- $n = 2p^e$ with an odd prime p , and $e \geq 1$
- $n = 2, 4$

This will be proven later. In particular, the most important case is that there *do* exist primitive roots modulo *primes*.

It is useful to make clear one important property of primitive roots:

Proposition: Let g be a primitive root modulo n . Let ℓ be an integer so that

$$g^\ell = 1 \pmod{n}$$

Then $\varphi(n)$ divides ℓ .

Proof: Using the Division Algorithm, we may write $\ell = q \cdot \varphi(n) + r$ with $0 \leq r < \varphi(n)$. Then

$$1 = g^\ell = g^{q \cdot \varphi(n) + r} = (g^{\varphi(n)})^q \cdot g^r = 1^q \cdot g^r = g^r \pmod{n}$$

Since g is a primitive root, $\varphi(n)$ is the least positive exponent so that g raised to that power is $1 \pmod{n}$. Thus, since $1 = g^r \pmod{n}$, it must be that $r = 0$. That is, $\varphi(n) | \ell$. ♣

11.3 Euler's criterion for square roots mod p

Fermat's Little Theorem gave some information about **square roots** modulo primes p . Now we will explain **Euler's criterion**, which gives a way to efficiently determine whether or not a given integer y has a square root modulo a prime p (presuming that we are acquainted with a fast exponentiation algorithm). To prove Euler's criterion we must grant the existence of **primitive roots** modulo primes, which will be proven only later.

Given y , a **square root** of y modulo m (with m not necessarily prime) is an integer x so that

$$x^2 \equiv y \pmod{m}$$

If there is such an x , then y is a **square mod m** , or, in archaic terminology, a **quadratic residue mod m** . If there is no such x , then y is a **non-square mod m** , or, in archaic terminology, a **quadratic non-residue mod m** .

Remark: As with multiplicative inverses, there is essentially no *tangible* connection between these square roots and square roots which may exist in the real or complex numbers. Thus, the expressions ' \sqrt{y} ' or ' $y^{1/2}$ ' have no intrinsic meaning for $y \in \mathbf{Z}/p$.

Example: Since $2^2 = 4 = -1 \pmod{5}$, 2 is a square root of -1 modulo 5. We would write

$$2 = \sqrt{-1} \pmod{5}$$

Note that the fact that there is no *real* number which is a square root of -1 is no argument against the existence of a square root of -1 modulo 5.

Example: Since $4^2 = 16 = 5 \pmod{11}$,

$$4 = \sqrt{5} \pmod{11}$$

Example: There is *no* $\sqrt{2}$ modulo 5: to be sure of this, we compute 5 cases:

$$\begin{aligned} 0^2 &= 0 \neq 2 \pmod{5} \\ 1^2 &= 1 \neq 2 \pmod{5} \\ 2^2 &= 4 \neq 2 \pmod{5} \\ 3^2 &= 9 = 4 \neq 2 \pmod{5} \\ 4^2 &= 16 = 1 \neq 2 \pmod{5} \end{aligned}$$

Since $\mathbf{Z}/5$ consists of just the 5 congruence classes $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$, we don't need to check any further to know that there is no square root of 2 modulo 5.

From a naive viewpoint, it would appear that the only way to check whether the square root of y modulo m exists is by *brute force*, squaring each element of \mathbf{Z}/m in turn to see if by chance the value y appears among the squares. From this viewpoint, it would be especially laborious to be sure that something had *no* square root, since all of \mathbf{Z}/m would have to be searched. But Fermat's Little Theorem (together with the *fast exponentiation* algorithm) gives some help here. But present we can only prove *half* the following theorem:

11.4 Euler's criterion for roots mod p

Just as in the case of square roots, there is a criterion (due to Euler) for whether or not an integer y can be an n^{th} power modulo a prime p , when $p \equiv 1 \pmod{n}$. By contrast, we've already seen that when $\gcd(n, p-1) = 1$, *everything* is an n^{th} power mod p . In the case of square roots a little more can be said, which is important in later discussion of *quadratic symbols* and the theorem on Quadratic Reciprocity.

Again, a non-zero y modulo p is an n^{th} -**power** (or, in archaic terminology, n^{th} -**power residue**) modulo p if there is x so that $x^n \equiv y \pmod{p}$. (If there is no such x , then y is an n^{th} -**power non-residue**.)

Theorem: (*Euler's Criterion*) Let p be a prime with $p \equiv 1 \pmod{n}$. Let y be relatively prime to p . Then y is an n^{th} power mod p if and only if $y^{(p-1)/n} \equiv 1 \pmod{p}$. As a special case, for odd primes p , for p not dividing y , y is a *non-zero square* mod p , if and only if $y^{(p-1)/2} \equiv 1 \pmod{p}$.

Remark: This is a reasonable test for *not* being a square mod p . Apparently Euler was the first to observe this, about 300 years ago. Also, later *Quadratic Reciprocity* will give another mechanism to test whether or not something is a square modulo p . The criterion for n^{th} powers has not replacement.

Proof: Easy half: Suppose that $y = x^n \pmod{p}$. Then, invoking Fermat's Little Theorem,

$$y^{(p-1)/n} = (x^n)^{(p-1)/n} = x^{p-1} = 1 \pmod{p}$$

as claimed.

Hard half: Now suppose that $y^{(p-1)/n} = 1 \pmod{p}$, and show that y is an n^{th} power. Let g be a *primitive root* modulo p , and let ℓ be a positive integer so that $g^\ell = y$. We have

$$(g^\ell)^{(p-1)/n} = 1 \pmod{p}$$

From the discussion of primitive roots above, this implies that

$$(p-1) \mid \ell \cdot (p-1)/n$$

(since $\varphi(p) = p - 1$ for prime p). By unique factorization in the ordinary integers, the only way that this can happen is that ℓ be divisible by n , say $\ell = kn$ for some integer k . Then

$$y = g^\ell = g^{kn} = (g^k)^n \pmod{p}$$

That is, y is the n^{th} power of g^k . ♣

Corollary: (*Euler's Criterion*) Let p be an odd prime. Let y be relatively prime to p . Then

$$y^{(p-1)/2} \equiv 1 \pmod{p} \text{ if } y \text{ is a square mod } p$$

and

$$y^{(p-1)/2} \equiv -1 \pmod{p} \text{ if } y \text{ is a non-square mod } p$$

Proof: The only new thing to prove, is that if y is a non-square then $y^{(p-1)/2} \equiv -1 \pmod{p}$. Since by Fermat's Little Theorem $y^{p-1} = 1 \pmod{p}$, certainly

$$(y^{(p-1)/2})^2 = 1 \pmod{p}$$

That is, $y^{(p-1)/2} \pmod{p}$ satisfies $x^2 = 1 \pmod{p}$, and it is not 1. Certainly -1 is one other solution to the equation $x^2 = 1 \pmod{p}$. If we can show that there are no other solutions to this equation than ± 1 , then we'll be done. Suppose x is an integer so that $x^2 = 1 \pmod{p}$. Then, by definition, $p|(x-1)(x+1)$.

We recall that since p is prime, if $p|ab$ then either $p|a$ or $p|b$. It might be good to review why this is true: suppose that $p|ab$ but p does not divide a , and aim to show that $p|b$. Let $ab = kp$. Since p is prime $\gcd(p, a) = 1$, so there are integers s, t so that $sp + ta = 1$. Then

$$b = b \cdot 1 = b \cdot (sp + ta) = bsp + tab = bsp + tkp = p \cdot (bs + tk)$$

Thus, $p|b$, as claimed.

Therefore, in the case at hand, if $p|(x-1)(x+1)$ then either $p|(x-1)$ or $p|(x+1)$. That is, as claimed, $x = \pm 1 \pmod{p}$. This completes the proof that $y^{(p-1)/2} = -1 \pmod{p}$ if and only if y is a non-square mod p (and relatively prime to p). ♣

#11.85 Is 2 a square modulo 101?

#11.86 Is 3 a square modulo 101?

#11.87 Is 2 a cube modulo 103?

#11.88 Is 3 a cube modulo 103?

#11.89 Is 2 a 7th power modulo 113?

#11.90 Is 15 a 7th power modulo 113?

12. (*) Public-Key Ciphers

- A little history
 - Trapdoors
 - The RSA cipher
 - The ElGamal cipher
-

12.1 A little history

Until about 1975, the only kinds of ciphers in existence were **symmetric ciphers**, meaning that knowledge of the encryption key would easily give knowledge of the decryption key, and *vice-versa*. These are also commonly called **secret-key ciphers**, since *all* of the keys involved have to be kept secret.

By contrast, a **public-key** or **asymmetric** cipher system is one in which knowledge of the encryption key gives essentially no clue as to the decryption key. Looking at all the classical symmetric ciphers certainly gives no inkling that a public-key cipher is even *possible*.

After some highly original (and unappreciated) work by Ralph Merkle, the general idea of a public-key cipher was first proposed in W. Diffie and W. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory IT-22 (1976), pp. 644-654. A public-key system based on the **knapsack problem** appeared in R. Merkle and M. Hellman, *Hiding information and signatures in trapdoor knapsacks*, IEEE Transactions on Information Theory IT-24 (1978), pp. 525-530. The latter system was “cracked”, and even though it has now been “fixed”, the loss of confidence in the knapsack problem seems irreversible. One of the most popular public-key systems is *RSA*, named after the authors: R.L. Rivest, A. Shamir, and L. Adleman: *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM 21 (1978), pp. 120-126. The security of RSA is based upon the difficulty of prime factorizations. The ElGamal system is a relative latecomer to the scene, appearing in T. El Gamal, *A public key cryptosystem and signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory IT-31 (1985), pp. 469-473.

The possibility of a public-key cipher system also gives rise to many applications that were previously inconceivable.

A simple example of the use of public key ciphers is in a **communications network**. For N people to communicate among each other using an *asymmetric* cipher such as RSA requires only N triples (e, d, n) : each individual publishes their public key, so to communicate securely with them *anyone* simply encrypts with the corresponding public key. That is, the whole communication network only requires one batch of information (e, d, n) *per person*. By contrast, a *symmetric* cipher would require a key *per pair of people*, which would require $N(N-1)/2$ for N people. Thus, using asymmetric ciphers greatly reduces the number of keys required to maintain a communications network. Using the $N(N-1)/2$ keys for a symmetric cipher set-up for a communication network involving N people, in which every *pair* of people has an encryption/decryption key pair, is not good. First, each person in the network must remember $N-1$ keys. Second, there are altogether $N(N-1)/2$ key pairs altogether, which have to be created and distributed.

Because the encryption and decryption algorithms for asymmetric ciphers are considerably slower than those for symmetric ciphers, in practice the asymmetric ciphers are used to securely exchange a **session key** for a symmetric cipher to be used for the actual communication. That is, the only plaintext encrypted with

the asymmetric cipher is the key for a symmetric cipher, and then the faster-running symmetric cipher is used for encryption of the actual message.

The trick of using *session keys* is by now very common in real uses of cryptography. Thus, in encryption for secrecy, the advantages of public-key ciphers can be realized while at the same time benefiting from the speed of symmetric ciphers. Further, in applications to new "exotic" protocols there is no replacement for public-key ciphers.

12.2 Trapdoors

Each asymmetric (public-key) cipher depends upon the *practical irreversibility* of some process, usually referred to as the **trapdoor**. At present, all the asymmetric ciphers believed to be reasonably secure make use of tasks from *number theory*, although in principle there are many other possibilities.

The RSA cipher uses the fact that, while it is not hard to compute the product $n = pq$ of two large primes p, q (perhaps $\approx 10^{80}$ or larger), to factor a very large integer $n \approx 10^{160}$ into its prime factors seems to be essentially impossible.

The El Gamal cipher uses the fact that, while exponentiation modulo large moduli m is not hard, computation of **discrete logs** is prohibitively difficult. That is, given x, e, p (with p prime) all $\approx 10^{140}$ or so, to compute $y = x^e \% m$ is not too hard. But, going the other direction, to compute the exponent e (the *discrete logarithm* of y base x modulo b) given y, x, p seems to be hard.

Note the qualifications in the last two paragraphs: we say that the tasks *seem to be* hard. At this time there is no *proof* that factorization into primes is *intrinsically* terribly hard. On the other hand, there is a great deal of practical evidence that this is a hard task: people have been thinking about this issue for hundreds of years, and more recently more intensely so because of its relevance to cryptology. The same is true of the discrete logarithm problem.

The earliest public-key cipher, that of Hellman-Merkle, had the opposite problem: while based upon a *provably* hard problem, the so-called *knapsack problem*, the modification necessary to make decoding possible fatally altered the problem so as to make it no longer hard!

In 1978, McEliece proposed a cipher based on algebraic coding theory. This used a *Goppa code* made to appear as a general *linear code*. The decoding problem for general linear codes is *provably* difficult ("NP-complete"), while the decoding problem for Goppa codes is "easy". This cipher does not seem to have been broken, but it is not as popular as RSA and ElGamal. The idea of "hiding" an easier problem inside an NP-complete problem is similar to the trick in Hellman-Merkle, which seems to have made some people nervous and suspicious of the security of the McEliece cipher.

So, in the end, although the problems haven't been *proven* hard, the *apparent practical difficulty* (after wide attention!) of the problems of factoring and taking discrete logs make RSA and ElGamal the most popular public-key ciphers.

The recently-publicized **elliptic-curve ciphers** are technical variants of these others. The description requires considerable further preparation.

12.3 The RSA cipher

The idea of this cipher is due to R.L. Rivest, A. Shamir, and L. Adleman: *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM 21 (1978), pp. 120-126. The key point is that factoring large numbers into primes is difficult. Perhaps surprisingly, merely testing large numbers for primality is much easier.

- The hard task
- Description of encryption and decryption
- Elementary aspects of security of RSA
- Speed of encryption/decryption algorithms
- Key generation and management
- Export regulations?!

The hard task

The hard task here is **factorization of large integers into primes**. Essential tasks which are *relatively* easy are:

- exponentiation $x^e \% n$ modulo n for $n > 10^{160}$ and for large exponents e .
- finding many large primes $p > 10^{80}$

As we will see, the contrast in apparent difficulties of these tasks is the basis for the security of the RSA cipher secure.

The difficulty of factoring large integers into primes is intuitively clear, although this itself is no proof of its difficulty. By contrast, it should be surprising that *we can test large numbers for primality without looking for their factors*.

The issue of efficiently evaluating large powers x^e of large integers x reduced modulo large integers n is more elementary.

And keep in mind that the relevant sizes $n > 10^{160}$ and $p > 10^{80}$ will have to be increased somewhat as computing speeds increase, even if no improvements in algorithms occur.

Description of encryption and decryption

There are two keys, e and d . Auxiliary information, which is not secret, consists of a large-ish integer n . (The nature of n , and the relation of e, d to each other and to n will be described below). A plaintext x is *encoded* first as a positive integer which we still call x , and for present purposes we require that $x < n$. Then the **encoding** step is

$$E_{n,e}(x) = x^e \% n$$

where $z \% n$ denotes the **reduction** of z modulo n . This produces a ciphertext $y = x^e \% n$ which is also a positive integer in the range $0 < y < n$. The **decryption** step is

$$D_{n,d}(y) = y^d \% n$$

That's it!

Of course, for the decryption step to *really decrypt*, the two keys e, d must have the property that

$$(x^e)^d \equiv x \pmod{n}$$

for all integers x (at least in the range $0 < x < n$). **Euler's Theorem** (below) asserts that if $\gcd(x, n) = 1$ then

$$x^{\varphi(n)} \equiv 1 \pmod{n}$$

where $\varphi(n)$ is the Euler phi-function evaluated at n , defined to be the number of integers ℓ in the range $0 < \ell \leq n$ with $\gcd(\ell, n) = 1$. Thus, the relation between e and d is that they are mutually **multiplicative inverses modulo** $\varphi(n)$, meaning that

$$d \cdot e \equiv 1 \pmod{\varphi(n)}$$

In that case, we can verify that the encryption-decryption really works for $\gcd(x, n) = 1$.

$$D_{n,d}(E_{n,e}(x)) = (x^e \% n)^d \% n = (x^e)^d \% n$$

since by now we know that reduction modulo n can be done whenever we feel like it, or *not*, in the course of an arithmetic calculation whose answer will be reduced modulo n at the end. By properties of exponents,

$$(x^e)^d \% n = x^{e \cdot d} \% n$$

Since $ed \equiv 1 \pmod{\varphi(n)}$, there is an integer ℓ so that

$$ed = 1 + \ell\varphi(n)$$

Then

$$x^{ed} = x^{1+\ell\varphi(n)} = x^1 \cdot (x^{\varphi(n)})^\ell \equiv x \cdot 1^\ell \equiv x \pmod{n}$$

by invoking Euler's theorem.

Note that we must assume that the plaintext x is **prime to** n . Since n is the product of the two large primes p and q , being relatively prime to n simply means *not* being divisible by either p or q . The probability that a "random" integer x in the range $0 \leq x \leq n$ would be divisible by p or q is

$$\frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$$

This is a very tiny number, so we *just ignore this possibility*.

The encryption exponent e (and decryption exponent d) must be prime to $\varphi(n) = (p-1)(q-1)$ so that so that it will have a multiplicative inverse modulo $\varphi(n)$, which will be the decryption exponent d .

A common chain of events is the following. Alice picks two large primes p and q (with $p \neq q$), and puts $n = pq$. The primes p and q must be kept secret. She then further picks the encryption and decryption exponents e and d so that $e \cdot d \equiv 1 \pmod{\varphi(n)}$. *She publishes the encryption exponent e on her web page, along with the modulus n .* Her decryption exponent d is kept secret also. Then anyone who wants to send email to Alice encrypted so that only Alice can read it can encrypt plaintext x by

$$E_{n,e}(x) = x^e \% n$$

Alice is the only person who knows the decryption exponent d , so she is the only one who can recover the plaintext by

$$x = D_{n,d}(E_{n,e}(x))$$

Since in this situation she can make the encryption key *public*, often the encryption key e is called the **public key** and the decryption key d is called the **private key**.

Elementary aspects of security of RSA

The security of RSA more or less depends upon the *difficulty of factorization of integers into primes*. This seems to be a genuinely difficult problem. But, more precisely, security of RSA depends upon a much more *special* problem, the difficulty of factoring numbers of the special form $n = pq$ (with p, q prime) into primes. It is conceivable that the more special problem could be solved by special methods not applicable to the general one. But for now the special-ness of the problem seems not to have allowed any particularly good specialized factorization attacks.

The reason that difficulty of factorization makes RSA secure is that for n the product of two big primes p, q (with the primes kept secret), it seems hard to compute $\varphi(n)$ when only n is given. Of course, once the prime factorization $n = p \cdot q$ is known, then it is *easy* to compute $\varphi(n)$ via the standard formula

$$\varphi(n) = \varphi(pq) = (p-1)(q-1)$$

If an attacker learns $\varphi(n)$, then the decryption exponent d can be relatively easily computed from the encryption exponent e , by using the **Euclidean Algorithm**, since the decryption exponent is just the multiplicative inverse of e modulo n .

In fact, we can prove that for numbers n of this special form, knowing both n and $\varphi(n)$ *gives* the factorization $n = p \cdot q$ (with very little computation). The trick is based on the fact that p, q are the roots of the equation

$$x^2 - (p+q)x + pq = 0$$

Already $pq = n$, so if we can express $p+q$ in terms of n and $\varphi(n)$, we will have the coefficients of this equation expressed in terms of n and $\varphi(n)$, giving an easy route to p and q separately.

Since

$$\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1$$

we can rearrange to get

$$p+1 = n - \varphi(n) + 1$$

Therefore, p and q are the roots of the equation

$$x^2 - (n - \varphi(n) + 1)x + n = 0$$

Therefore, the two roots

$$\frac{-(n - \varphi(n) + 1) \pm \sqrt{(n - \varphi(n) + 1)^2 - 4n}}{2}$$

are p and q .

And we must note that it is conceivable that there is some other way to obtain the plaintext, or some portion of it, without factoring n .

It might seem that knowledge of the encryption and decryption exponents e, d would not yield the prime factorization $n = p \cdot q$. Thus, it might *seem* that even if the pair e, d is *compromised*, in the sense that both numbers become known to an adversary, the utility of the number $n = p \cdot q$ is not gone. However, in fact *disclosure of the private (decryption) key compromises the cipher*. Specifically, there is a Las Vegas algorithm that runs “quickly” which will yield the factorization $n = pq$.

Note that none of the *users* of a system with modulus n (the product of two secret primes p, q), public key e , and private key d *do not need to know the primes* p, q . Therefore, it would be possible for a **central**

agency to use the same modulus $n = pq$ over and over. However, as just noted, compromise of one key pair compromises the others.

Speed of encryption/decryption algorithms

If done naively, raising large numbers to large powers takes a long time. Such exponentiation is required by both encryption and decryption in the RSA, so from a naive viewpoint it may be unclear why the algorithms themselves are any easier to execute than a hostile attack. But, in fact, the required exponentiation can be arranged to be much faster than prime factorizations for numbers in the relevant range (with a hundred or more digits). Even so, at this time it seems that the RSA encryption and decryption algorithms (and *most* asymmetric cipher algorithms) run considerably more slowly than the best *symmetric* cipher algorithms.

Typically the primes p, q are chosen to have a hundred digits or so. Therefore, even if the encryption exponent e is chosen to be relatively small, perhaps just a few decimal digits, the multiplicative inverse (the decryption key) will be about as large as n . Thus, the task of computing large powers of integers, modulo a large n , must be executable relatively quickly by comparison to the task of *factoring* n .

There is an important elementary speed-up of exponentiation we'll describe below, which allows us to consider exponentiation "easy". This algorithm is useful for computing powers of numbers or other algebraic even more generally. That is, to compute x^e we do *not* compute $x^1, x^2, x^3, x^4, x^5, \dots, x^{e-1}, x^e$.

Key generation and management

To set up a modulus $n = pq$ from secret primes p, q , and to determine a key pair e, d with $ed \equiv 1 \pmod{1}$, requires first of all two large primes p, q , at least $> 10^{80}$, for example. Since the security of RSA is based upon the intractability of factoring, it is very lucky that *primality testing is much easier than factorization into primes*. That is, we are able to obtain many "large" primes $p, q > 10^{80}$ *cheaply*, despite the fact that we cannot generally factor "large" numbers $n = pq > 10^{160}$ into primes (even with good algorithms).

The *decryption* (or *private*) key d can be chosen first, after p, q . For there to be a corresponding *encryption* key e it must be that d is relatively prime to $(p-1)(q-1)$, and then the Euclidean Algorithm gives an efficient means to compute e .

One way to obtain d relatively prime to $(p-1)(q-1)$ is simply by *guessing and checking*, as follows. Note that since $p-1$ and $q-1$ themselves are large we may not have their prime factorizations! We pick a random large *prime* d , and then use the Euclidean Algorithm to find the greatest common divisor of this d and $(p-1)(q-1)$. If the *gcd* is > 1 we just guess again. Since d was a large random *prime* the heuristic probability is very high that there first guess itself will already be relatively prime to $(p-1)(q-1)$.

Further technical notes:

- In many implementations, to make encryption easy, the *encryption* exponent is always taken to be just 3, and the primes p, q *not* congruent to 1 modulo 3. This certainly offers further simplifications.
- For technical reasons, some people have more recently recommended

$$2^{16} + 1 = 65537$$

(which is prime) as encryption exponent. Then take the primes p, q *not* congruent to 1 modulo 65537.

- Both $p-1$ and $q-1$ should have at least one very large prime factor, since there are factorization attacks against $n = pq$ that are possible if $p-1$ or $q-1$ have only smallish prime factors.

- The primes p and q should not be “close” to each other, since there are factorization attacks on n that succeed in this case (Fermat, Pollard’s rho, etc).
- Don’t want the ratio p/q to be “close” to a rational number with smallish numerator and denominator, since then D.H. Lehmer’s Continued Fraction factorization attack on $n = pq$ will succeed.

U.S. export regulations

As of this writing (December 1997), export of RSA software with any keysize is allowed for **authentication** purposes, although it must be demonstrated that the product in question cannot easily be converted to use for encryption. For RSA used for encryption, evidently the keysize must be limited to 512 bits. Export of encryption for financial use with larger key sizes is sometimes allowed: for example, Cybercash has been allowed to export 768-bit keys for financial transactions.

Probably the RSA FAQ is the best reference for the current status of export and other practical questions about RSA:

- <http://www.rsa.com/rsalabs/newfaq/>

12.4 The ElGamal cipher

This idea appeared in T. El Gamal, *A public key cryptosystem and signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory IT-31 (1985), pp. 469-473. This idea is a little more complicated than RSA, but still essentially elementary. The idea also lends itself to certain technical generalizations more readily than does RSA. For example, the elliptic curve cryptosystems are analogues of the ElGamal cipher.

- The hard task
- Description of encryption and decryption
- Elementary aspects of security of ElGamal
- Speed of encryption/decryption algorithms
- Key generation and management

The hard task

The hard task here is **computation of discrete logs**. This means the following. Fix a modulus m , and integers b, c . An integer solution x to the equation

$$b^x \equiv c \pmod{m}$$

is a **(discrete) logarithm base b of c modulo m** . It is important to know that for random m, b , and c there may be no such x . But for prime modulus p and good choice of base b there will exist discrete logarithm for any c not divisible by p . (These theoretical aspects will be clarified later.)

Fix a large prime $p > 10^{150}$. For two integers b, c suppose that we know that

$$b^x = c \pmod{p}$$

for some x . The difficult task is to compute x given only b, c, p .

For any positive integer m , an integer b is usually called a **primitive root modulo p** if every integer c relatively prime to p may be expressed in the form

$$c = b^x \pmod{m}$$

We will see later that there exist primitive roots mod m only for special sorts of integers, including mainly *prime* moduli. For prime modulus p , we will see that a primitive root $b \pmod{p}$ has the property that the smallest positive power b^k of b congruent to 1 modulo p is $p - 1$. That is,

$$b^{p-1} \equiv 1 \pmod{p}$$

and no smaller power will do. More generally, for arbitrary x relatively prime to a modulus divisible by prime m , the **order** or **exponent** of $x \pmod{m}$ is the smallest positive integer exponent n so that

$$x^n \equiv 1 \pmod{m}$$

We will see that primitive roots have *maximal* order.

For El Gamal it is not strictly necessary to have a primitive root modulo p , since we only need the configuration $b^\ell \equiv c \pmod{p}$, but we must require that the *order* of $b \pmod{p}$ is close to the maximum possible, or else the cipher can be too easily broken.

Both the idea of “discrete logarithm” and the use of the difficulty of computing discrete logarithms to construct a cryptosystem admit further abstraction. The most popular example of such a generalization is the **elliptic curve cipher**, which needs considerable preparation even to *describe*. We will do this later.

Description of encryption and decryption

Fix a large prime $p > 10^{150}$, a primitive root b modulo p (meaning that any y can be expressed as $y = b^L \pmod{p}$), and an integer c in the range $1 < c < p$. The *secret* is the power ℓ (the **discrete logarithm**) so that $b^\ell = c \pmod{p}$. Only the *decryptor* knows ℓ .

The **encryption step** is as follows. A plaintext x is encoded as an integer in the range $0 < x < p$. The encryptor chooses an auxiliary random integer r , which is a *temporary secret known only to the encryptor*, and encrypts the plaintext x as

$$y = E_{b,c,p,r}(x) = (x \times c^r) \% p$$

Along with this encrypted message is sent the “header” b^r . Note that the encryptor only needs to know b, c, p and chooses random r , but does not know the discrete logarithm ℓ .

The decryption step requires knowledge of the discrete logarithm ℓ , but not the random integer r . First, from the “header” b^r the decryptor computes

$$(b^r)^\ell = b^{r \cdot \ell} = (b^\ell)^r = c^r \pmod{p}$$

Then the plaintext is recovered by multiplying by the multiplicative inverse $(c^r)^{-1}$ of c^r modulo p :

$$D_{b,c,p,r,\ell}(y) = (c^r)^{-1} \cdot y \% p = (c^r)^{-1} \cdot c^r \cdot x \pmod{p} = x \% p$$

Elementary aspects of security of ElGamal

The security of this cipher depends upon the difficulty of computing the **discrete logarithm** ℓ of an integer c **base** b , modulo prime p . Again, this is an integer so that

$$b^\ell = c \pmod{p}$$

There seems to be little tangible connection between this notion of logarithm and logarithms of real or complex numbers, although they do share some abstract properties.

The naive algorithm to compute a discrete logarithm is simply trial and error. Better algorithms to compute discrete logarithms, to attack the El Gamal cipher for example, require more understanding of integers modulo p .

To avoid **logarithm computation attacks**, we would also want to choose p so that $p - 1$ does not have “too many” small prime factors. Since $p - 1$ is even, it will always have a factor of 2, but beyond this we hope to avoid small factors. This can be made more precise later.

Speed of encryption/decryption algorithms

As with RSA, the speed of encryption and decryption is mainly dependent upon speed of exponentiation modulo n , which can be made reasonably fast.

A feature of ElGamal (and related algorithms) is that encryptors need a good supply of random numbers. Thus, availability of high-quality pseudo-random number generators is relevant to ElGamal.

Comments on key generation and management

The most obvious requirement for this cipher system is a generous supply of large primes p , meaning $p > 10^{160}$ or so. The naive trial division primality test is completely inadequate for this.

Whoever creates the configuration

$$b^\ell \equiv c \pmod{p}$$

will presumably first choose a large prime p , most likely meeting some further technical conditions. An especially nice kind of prime, for this and many other purposes, is of the form

$$p = 2 \cdot p' + 1$$

where p' is another prime. In that case, about half the numbers b in the range $1 < b < p - 1$ are primitive roots (so have order $2p'$) and the other half have order p' , which is still not so bad. Thus, random selection of such b gives a good candidate. Random choice of the exponent ℓ , and computation of $c = b^\ell \% p$ completes the preparations.

In the case that the prime p is of the special form $2p' + 1$ with p' prime, it is easy to find primitive roots in any case, since (as we will see later) the elements of orders p' (rather than $2p'$ which a primitive root would have) are all **squares** in \mathbf{Z}/p . The property of being a square or not is easily computable by using Legendre and Jacobi quadratic symbols, as we will see. Thus, it is quite feasible to require that the number b used in El Gamal be a primitive root for primes $p = 2p' + 1$.

It is plausible to use a single prime modulus p for several key configurations $b^\ell = c \pmod{p}$ since there are many different primitive roots modulo p , but we will see that compromise of one such configuration compromises others.

Also, any encryptor will need a good supply of (pseudo-) random integers for the encryption process. This is an issue in itself.

13. (*) Pseudoprimes and Primality Tests

The simplest test for primality, the **trial division** method, may require roughly \sqrt{n} steps to prove that n is prime. This already takes several minutes on a 200 Mhz machine when $n \approx 10^{18}$, so would take about 10^{16} years for $n \approx 10^{60}$. Yet modern ciphersystems need *many* primes at least 10^{60} , if not larger.

The first compromise is that we can gain enormously in *speed* if we sacrifice *certainty*. That is, we can quickly prove that very large numbers are *likely* to be prime, but will not have the absolute certainty of primality that traditional computations would give. But, since those traditional computations could never be completed, perhaps the idea that something is being “sacrificed” is incorrect.

Numbers which are not truly known to be prime, but which have passed various probabilistic tests for primality, are called **pseudoprimes** (of various sorts). Sometimes the word “pseudoprime” is used to indicate a *non-prime* which has nevertheless passed a probabilistic test for primality. For us, though, a pseudoprime is simply a number (which may or may not really be prime) which has passed some sort of probabilistic primality test.

Each of these yet-to-be-specified probabilistic primality tests to be performed upon a number n makes use of one or more auxiliary numbers b , chosen “at random” from the range $1 < b < n$. If a particular auxiliary b tells us that “ n is likely prime”, then b is a **witness** to the primality of n . The problem is that a significant fraction of the numbers b in the range $1 < b < n$ may be **false witnesses** (sometimes called **liars**), meaning that they tell us that n is prime when it's *not*.

Thus, part of the issue is to be sure that a large fraction of the numbers b in the range $1 < b < n$ are (“true”) witnesses to either the primality or compositeness of n .

The fatal flaw in the Fermat pseudoprime test is that there are composite numbers n for which there are *no* witnesses. These are called **Carmichael numbers**. The other two primality tests have no such flaw.

In all cases, the notion of *probability* that we use in saying something such as “ n is prime with probability 2^{-10} ” is a fundamentally *heuristic* one, based on the doubtful hypothesis that among n possibilities *which we don't understand* each has probability $1/n$ of occurring. (This sort of pseudo-probabilistic reasoning has been rightfully disparaged for over 200 years.)

On the other hand, these probabilistic primality tests can be converted to *deterministic* tests if the **Extended Riemann Hypothesis** is true. Many mathematicians believe that the Extended Riemann Hypothesis is true, and there is no simple evidence to the contrary (as of early 1998), but it seems that no one has any idea how to *prove* it, either. The question has been open for about 140 years, with no real progress on it. Assuming that the Extended Riemann Hypothesis is true, it would follow that there is a universal constant C so that for any number n , if n is composite then there is an *Euler witness* (and also a *strong witness*) b with

$$1 < b < C \cdot (\log n)^2$$

That is, we wouldn't have to look too far to find a (truthful) witness if n is composite.

- Fermat pseudoprimes
- Euler pseudoprimes
- Strong pseudoprimes
- Miller-Rabin primality test

13.1 Fermat pseudoprimes

This section gives a heuristic test for primality. It has several weaknesses, and in the end is not what we will use, but it illustrates two very interesting points: first, that *probabilistic* algorithms may run much faster than deterministic ones, and, second, that we simply can't expect to provide proofs for everything which seems to be true.

On one hand, Fermat's so-called *Little Theorem* asserts that for any prime number p and integer b

$$b^p = b \pmod{p}$$

Equivalently, for p not dividing b , we have

$$b^{p-1} = 1 \pmod{p}$$

This is a special case of Euler's theorem which asserts that for b prime to an integer n ,

$$b^{\varphi(n)} = 1 \pmod{n}$$

where φ is Euler's phi-function. (Euler's theorem is best proven using a little *group theory*, and we will do this later).

An integer n is called a **Fermat pseudoprime** or **ordinary pseudoprime** or simply **pseudoprime** if

$$2^{n-1} = 1 \pmod{n}$$

No, there is no assurance that n 's being a Fermat pseudoprime implies that n is prime, since there is no converse to Fermat's little theorem. Yet, *in practice* it is "very unusual" that $2^n = 2 \pmod{n}$ and yet n is not prime. Specifically, $341 = 11 \times 31$ is not prime, and is the first non-prime number which is a Fermat pseudoprime: $2^{341} = 2 \pmod{341}$. The next few non-prime Fermat pseudoprimes are

$$561, 645, 1105, 1387, 1729, 1905, 2047, 2465$$

There are only 5597 non-prime Fermat pseudoprimes below 10^9 .

It *is* true that if an integer n fails the Fermat test, meaning that $2^{n-1} \not\equiv 1 \pmod{n}$, then n is certainly *not* a prime (since, if it *were* prime, then $2^{n-1} = 1 \pmod{p}$, after all!).

Since the fast exponentiation algorithm provides an economical method for computing $b^{n-1} \pmod{p}$, *we can test whether an integer n is a Fermat pseudoprime much faster than we can test it for primality by trial division.*

We can make a more stringent condition: an integer n is a **Fermat pseudoprime base b** if

$$b^{n-1} = 1 \pmod{n}$$

If $b^{n-1} \not\equiv 1 \pmod{n}$, then n is certainly *not* a prime. On the other hand, even if $b^{n-1} = 1 \pmod{n}$ for all b relatively prime to n , we have no assurance that n is prime.

An integer b in the range $1 < b < n - 1$ so that $b^{n-1} \equiv 1 \pmod{n}$ is a **(Fermat) witness** for the primality of n . If n isn't actually prime, then that b is a (Fermat) **false witness** or (Fermat) **liar**.

And the behavior of a non-prime can be different with respect to different bases. For example, the non-prime $91 = 7 \cdot 13$ is *not* a Fermat pseudoprime (base 2), but *is* a Fermat pseudoprime base 3.

Again, in practice, it is very unusual for an integer to be a pseudoprime base b for one or more bases b and yet fail to be a prime. For example, among integers under 46,000, the only Fermat pseudoprimes base

2 which are *not* prime are the 52 numbers 341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911, 10261, 10585, 11305, 12801, 13741, 13747, 13981, 14491, 15709, 15841, 16705, 18705, 18721, 19951, 23001, 23377, 25761, 29341, 30121, 30889, 31417, 31609, 31621, 33153, 34945, 35333, 39865, 41041, 41665, 42799.

Compare this to the fact that there are 4761 primes under 46,000. Thus, the failure rate for Fermat pseudoprime base 2 is only about one percent.

In that same range, the only non-prime Fermat pseudoprimes base 3 are the 35 numbers 91, 121, 671, 703, 949, 1541, 1891, 2665, 3281, 3367, 3751, 4961, 5551, 7107, 7381, 8205, 8401, 11011, 12403, 14383, 15203, 15457, 16471, 16531, 19345, 23521, 24661, 24727, 28009, 29161, 30857, 31697, 32791, 38503, 44287.

The only non-primes under 46,000 which are Fermat pseudoprimes *both* base 2 and base 3 are the 14 numbers 561, 1105, 1729, 2465, 2701, 2821, 6601, 8911, 10585, 15841, 18721, 29341, 31621, 41041. Thus, the failure rate here is less than a third of one percent.

Nevertheless, there are infinitely many integers which are pseudoprimes to all bases (relatively prime to them), and yet are not prime. These are called **Carmichael numbers**. Under 46,000, there are only 14 Carmichael numbers: 561, 1105, 1729, 2465, 2701, 2821, 6601, 8911, 10585, 15841, 18721, 29341, 31621, 41041.

There are “only” 2163 Carmichael numbers below 10^9 , and 8241 Carmichael numbers below 10^{12} , 19,279 up to 10^{13} , 44,706 up to 10^{14} , and 105,212 up to 10^{15} . (see R.G.E. Pinch, *The Carmichael numbers up to 10^{15}* , Math. Comp. 61 (1993), pp. 381-391.)

Later, we will show that *a Carmichael number must be odd, square-free, and be divisible by at least 3 primes*. This result is also necessary to understand why the *better* versions of “pseudoprime” and corresponding probabilistic primality tests (below) do not have failings analogous to the presence of Carmichael numbers.

It was an open problem for more than 80 years to determine whether there are or are not infinitely many Carmichael numbers. Rather recently, it was proven that there are infinitely-many: in fact, there is a constant C so that the number of Carmichael numbers less than x is $\geq C \cdot x^{2/7}$. See W.R. Alford, A. Granville, and C. Pomerance, *There are infinitely-many Carmichael numbers*, Ann. of Math. 140 (1994), pp. 703-722.

13.2 Strong pseudoprimes

Continuing with the use of square roots to test primality, we can go a bit further than Euler’s criterion. Here the underlying idea is that if p is a prime then \mathbf{Z}/p should have only 2 square roots of 1, namely ± 1 .

Let n be an *odd* number, and factor

$$n - 1 = 2^s \cdot \ell$$

with ℓ odd. Then n is a **strong pseudoprime** base b if

$$\text{either } b^\ell = 1 \pmod{n} \quad \text{or} \quad b^{2^r \cdot \ell} = -1 \pmod{n} \quad \text{for some } 0 \leq r < s$$

On the face of it, it is certainly hard to see how this is related to primality. And despite the remark just above about this test being related to the presence of “false” square roots of 1, it’s certainly not so clear why or how that works, either.

Nevertheless, granting fast exponentiation, the algorithm runs pretty fast. We’ll address the *how* and *why* issues later.

13.3 Miller-Rabin primality test

The Miller-Rabin probabilistic primality test hunts for *strong pseudoprimes*. When applied to a number n it tests whether n is an *Euler pseudoprime* base b for several different bases b . This test is easy to implement, so gets used in real life. The fact that makes it reasonably fast is that exponentiation modulo n is reasonably fast.

The *idea* of the test is that for non-prime n there will be at least 2 elements x of \mathbf{Z}/n with the property that $x^2 = 1$ by $x \neq \pm 1$. As with the Solovay-Strassen test, much further explanation is needed to see *why* it works, etc. The *operation* of the Miller-Rabin test itself is quite simple, though, even simpler than that of the Solovay-Strassen test.

As with the Solovay-Strassen test, this test can prove compositeness with *certainty*, but only proves primality with a certain *probability*.

Let n be a positive odd integer. Find the largest power 2^r dividing $n - 1$, and write $n - 1 = 2^r \cdot s$. In order to discover either

- n is composite *with certainty* or
- n is prime with probability $> 1 - (1/4)^k$

choose k “random” integers b in the range $1 < b < n - 1$.

For each b in the list, compute $b_1 = b^s \% n$. $b_2 = b_1^2 \% n$, $b_3 = b_2^2 \% n$, $b_{r+1} = b_r^2 \% n$. For the first index i so that $b_i = 1$ (if there *is* one), look at b_{i-1} . If $b_{i-1} \not\equiv -1 \pmod n$, then n is *surely composite*.

If for *every* b in the list the first index i with $b_i = 1$ has the property that $b_{i-1} \equiv -1 \pmod n$, then we imagine that n is *prime* with probability $> 1 - (3/4)^k$.

If *no* $b_i = 1$, then n is *surely composite*.

The idea is that if n is composite then at least $3/4$ the integers b in the range $1 < b < n - 1$ are *witnesses* to this fact.

Note that if *none* of the b_i is 1, then $b^{n-1} \neq 1$, so n is not a Fermat pseudoprime base b .

As with the Solovay-Strassen test, to demonstrate the presence of so many witnesses requires preparation, so we postpone it.

#13.91 The numbers 341, 561, 645, 1105 are all Fermat pseudoprimes base 2, but are not prime. Which false primes are detected by Fermat’s test base 3? Base 5?

#13.92 Find the smallest Euler (Solovay-Strassen) witnesses to the compositeness of the Carmichael numbers 561, 1105, 1729.

#13.93 Find the smallest strong (Miller-Rabin) witness to the compositeness of the Carmichael numbers 2465, 2821.

14. Vectors and matrices

The first version of **vector** one sees is that a vector is a **row** or **column** of numbers:

$$(x_1 \quad x_2 \quad \dots \quad x_n) \quad \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Vectors of the same size have a **vector addition**

$$(x_1 \quad x_2 \quad \dots \quad x_n) + (y_1 \quad y_2 \quad \dots \quad y_n) = (x_1 + y_1 \quad x_2 + y_2 \quad \dots \quad x_n + y_n)$$

and

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

There is also **scalar multiplication**

$$s \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} sx_1 \\ x_2 \\ \vdots \\ sx_n \end{pmatrix}$$

These operations in themselves are unremarkable and easy to execute.

Likewise, an m -by- n **matrix** is just an m -by- n block of numbers

$$x = \begin{pmatrix} x_{11} & x_{12} & x_{13} & \dots & x_{1n} \\ x_{21} & x_{22} & x_{23} & \dots & x_{2n} \\ x_{31} & x_{32} & x_{33} & \dots & x_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ x_{m1} & x_{m2} & x_{m3} & \dots & x_{mn} \end{pmatrix}$$

The entry in the i th row and j th column is called the (i, j) th *entry*. If x is the whole matrix, often its (i, j) th entry is denoted by subscripts

$$x_{ij} = (i, j)\text{th entry of the matrix } x$$

The **matrix addition** is the straightforward entry-by-entry addition of *two matrices of the same size*:

$$\begin{aligned} & \begin{pmatrix} x_{11} & x_{12} & x_{13} & \dots & x_{1n} \\ x_{21} & x_{22} & x_{23} & \dots & x_{2n} \\ x_{31} & x_{32} & x_{33} & \dots & x_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ x_{m1} & x_{m2} & x_{m3} & \dots & x_{mn} \end{pmatrix} + \begin{pmatrix} y_{11} & y_{12} & y_{13} & \dots & y_{1n} \\ y_{21} & y_{22} & y_{23} & \dots & y_{2n} \\ y_{31} & y_{32} & y_{33} & \dots & y_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ y_{m1} & y_{m2} & y_{m3} & \dots & y_{mn} \end{pmatrix} \\ &= \begin{pmatrix} x_{11} + y_{11} & x_{12} + y_{12} & x_{13} + y_{13} & \dots & x_{1n} + y_{1n} \\ x_{21} + y_{21} & x_{22} + y_{22} & x_{23} + y_{23} & \dots & x_{2n} + y_{2n} \\ x_{31} + y_{31} & x_{32} + y_{32} & x_{33} + y_{33} & \dots & x_{3n} + y_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ x_{m1} + y_{m1} & x_{m2} + y_{m2} & x_{m3} + y_{m3} & \dots & x_{mn} + y_{mn} \end{pmatrix} \end{aligned}$$

The **additive identity** or **zero matrix** $0_{m,n}$ of size m -by- n is the m -by- n matrix with all entries 0. It has the obvious property that if it is added to any other matrix x of that same shape we just get

$$x + 0_{m,n} = x = 0_{m,n} + x$$

There is also **matrix multiplication**, whose meaning and computation is more complicated: for a k -by- m matrix x and an m -by- n matrix y the (i, j) th entry of the product xy depends only upon the i th row of x and the j th columns of y : it is

$$\begin{aligned} \begin{pmatrix} \dots & \dots & \dots \\ \dots & (xy)_{ij} & \dots \\ \dots & \dots & \dots \end{pmatrix} &= \begin{pmatrix} x_{i1} & x_{i2} & x_{i3} & \dots & x_{im} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix} \begin{pmatrix} \dots & y_{1j} & \dots \\ \dots & y_{2j} & \dots \\ \dots & y_{3j} & \dots \\ \dots & \vdots & \dots \\ \dots & y_{mj} & \dots \end{pmatrix} \\ &= \begin{pmatrix} \dots & \dots & \dots \\ \dots & x_{i1}y_{1j} + x_{i2}y_{2j} + \dots + x_{im}y_{mj} & \dots \\ \dots & \dots & \dots \end{pmatrix} \end{aligned}$$

That is, the (i, j) th entry of the product is

$$(xy)_{ij} = x_{i1}y_{1j} + x_{i2}y_{2j} + \dots + x_{im}y_{mj} = \sum_{1 \leq \ell \leq m} x_{i\ell} y_{\ell j}$$

The (multiplicative) **identity matrix** 1_n of size n -by- n is the matrix

$$1_n = \begin{pmatrix} 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ & & & \dots \\ & & & 1 & 0 \\ & \dots & 0 & 1 \end{pmatrix}$$

with all 1's on the **diagonal** (from upper left to lower right) and 0's everywhere else. This has the property that it's name suggests: for any m -by- n matrix x and/or n -by- m matrix y , we have

$$x \cdot 1_n = x \quad 1_n \cdot y = y$$

Since the product of a k -by- m matrix x and an m -by- n matrix is k -by- n , we note that for each positive integer n the collection of n -by- n *square matrices* has both addition and multiplication which give outcomes back in the same collection.

Some n -by- n matrices x have a **multiplicative inverse** x^{-1} , meaning that

$$x \cdot x^{-1} = 1_n = x^{-1} \cdot x$$

Such square matrices are said to be **invertible**.

#14.94 Show that the inverse of the matrix $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ is $\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}$.

#14.95 Show that the inverse of the matrix $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$ is $\begin{pmatrix} 1 & 0 \\ -x & 1 \end{pmatrix}$.

#14.96 Show that the inverse of the matrix

$$\begin{pmatrix} 1 & x & x^2/2 \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}$$

is

$$\begin{pmatrix} 1 & -x & x^2/2 \\ 0 & 1 & -x \\ 0 & 0 & 1 \end{pmatrix}$$

#14.97 Show that the inverse of the matrix $\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}$ is $\begin{pmatrix} r^{-1} & 0 \\ 0 & 1 \end{pmatrix}$.

#14.98 Show that the matrix

$$\begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix}$$

does not lie in $GL(2, \mathbf{R})$, that is, has no multiplicative inverse.

#14.99 Find two 2-by-2 integer matrices A, B which do not commute, that is, so that $AB \neq BA$.

#14.100 Prove by induction that for any positive integer N

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^N = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$$

#14.101 Let

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Determine a formula for x^N for positive integers N , and prove (by induction) that it is correct.

15. Motions in two and three dimensions

One very important use of vectors and matrices is to give analytical and quantitative descriptions of basic manipulations of two-dimensional and three-dimensional objects. This makes possible computation by hand or by machine, rather than seeming to require precise drawing or visualization. In fact, these computations *are* what a person or machine has to do in order to create graphics.

First, recall that in analytic geometry an ordered pair of real numbers (x, y) refers to a point in the plane, while an ordered triple (x, y, z) refers to a point in three-space. For present purposes, in all matrix and vector computations we will write vectors as “**column vectors**” (rather than “row vectors”):

$$(x, y) = \begin{pmatrix} x \\ y \end{pmatrix}.$$
$$(x, y, z) = \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

We will write the **inner product** or **scalar product** or **dot product** of two two-dimensional vectors $v_1 = (x_1, y_1)$ and $v_2 = (x_2, y_2)$ as

$$\langle v_1, v_2 \rangle = x_1 x_2 + y_1 y_2$$

We will use the same notation for the inner product of two three-dimensional vectors $v_1 = (x_1, y_1, z_1)$ and $v_2 = (x_2, y_2, z_2)$ as

$$\langle v_1, v_2 \rangle = x_1 x_2 + y_1 y_2 + z_1 z_2$$

And the **length** of a two-dimensional vector $v = (x, y)$ is

$$\|v\| = \sqrt{\langle v, v \rangle} = \sqrt{x^2 + y^2}$$

and of a three-dimensional vector $v = (x, y, z)$ is

$$\|v\| = \sqrt{\langle v, v \rangle} = \sqrt{x^2 + y^2 + z^2}$$

The **distance** between two points v_1 and v_2 is

$$\text{distance from } v_1 \text{ to } v_2 = \|v_1 - v_2\|$$

Consider now two line segments with a common vertex: for three points v_o, v_1, v_2 , let s_1 be the line segment connecting v_o to v_1 , and let s_2 be the line segment connecting v_o to v_2 . Then

$$\text{cosine of angle between } s_1 \text{ and } s_2 = \frac{\langle v_1 - v_o, v_2 - v_o \rangle}{\|v_1 - v_o\| \cdot \|v_2 - v_o\|}$$

In particular, the two line segments are **perpendicular** (*orthogonal*) if and only if $\langle v_1 - v_o, v_2 - v_o \rangle = 0$.

All the “**motions**” we consider will be **functions** from the plane (two-space) to itself, or from three-space to itself. Thus, to describe a “motion” is to describe where each point goes, probably by a formula.

The first example is **rotations in the plane**. We wish to give an analytical or formulaic description of the operation of rotation counter-clockwise by amount θ , with the rotation being *around the origin*. Let R_θ be the matrix

$$R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

Define

$$f(x, y) = (x', y')$$

where

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = R_\theta \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

If one draws a picture (!) it will be visible that this function rotates everything by angle θ counter-clockwise around the origin.

The second example is **translations** in the plane. The translation by amount (h, k) is

$$f(x, y) = (x + h, y + k)$$

If $f(x, y)$ is written as a column vector, then this can be rewritten as

$$f(x, y) = \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} h \\ k \end{pmatrix}.$$

Thus, representing a point $v = (x, y)$ as a column vector, a rotation by angle θ is the function $v \rightarrow R_\theta v$ with R_θ as above. Representing (x_o, y_o) as a column vector v_o , translation by v_o is the function $v \rightarrow v + v_o$.

In three space, **translations** are still easy to describe: for a fixed amount (vector) $v_o = (x_o, y_o, z_o)$ to translate, the translation-by- v_o function sends a vector $v = (x, y, z)$ to

$$f(x, y, z) = v + v_o = \begin{pmatrix} x \\ y \\ z \end{pmatrix} + \begin{pmatrix} x_o \\ y_o \\ z_o \end{pmatrix}.$$

In three space, there are many more possible axes about which to rotate, although all rotations fixing the origin are of the form

$$f(x, y, z) = R \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

for some suitable 3-y-3 matrix R . In particular, for a rotation by angle θ around the z -axis we use

$$R = R_\theta^{(z)} = \begin{pmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

For a rotation around the y -axis we use

$$R = R_\theta^{(y)} = \begin{pmatrix} \cos \theta & 0 & -\sin \theta \\ 0 & 1 & 0 \\ \sin \theta & 0 & \cos \theta \end{pmatrix}$$

And for a rotation around the x -axis we use

$$R = R_\theta^{(x)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{pmatrix}$$

Without quite giving *general* definition of *rotation* in three-space, we nevertheless can state an important fact: every “rotation” in three-space fixing the origin $(0, 0, 0)$ can be (essentially uniquely) expressed as a composite

$$R_\alpha^{(x)} \circ R_\beta^{(y)} \circ R_\gamma^{(z)}$$

The angles α, β, γ are the **Euler angles** of the rotation.

#15.102 From the fact that left multiplication of a vector $\begin{pmatrix} x \\ y \end{pmatrix}$ by the matrix

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

corresponds to rotation of the point (x, y) by angle θ , prove the **Addition Laws** (so-called) for sine and cosine:

$$\cos(\alpha + \beta) = \cos \alpha \cos \beta - \sin \alpha \sin \beta$$

$$\sin(\alpha + \beta) = \cos \alpha \sin \beta + \sin \alpha \cos \beta$$

#15.103 In two-space (the plane), find a translation f_1 and a rotation f_2 in two-space so that $(f_1 \circ f_2)(1, 0) = (3, 4)$ and $(f_1 \circ f_2)(0, 1) = (4, 5)$.

#15.104 In two-space (the plane), find a rotation f_1 and a translation f_2 in two-space so that $(f_1 \circ f_2)(1, 0) = (3, 4)$ and $(f_1 \circ f_2)(0, 1) = (4, 5)$.

#15.105 Show that rotations in two-space preserve distances between points, and preserve angles between line segments sharing a common vertex.

#15.106 Show that translations in two-space preserve distances between points, and preserve angles between line segments sharing a common vertex.

#15.107 Let v_o be a vector in two-space, and let θ be an angle. Show that counter-clockwise rotation by θ , followed by translation by v_o , followed by counter-clockwise rotation by $-\theta$, is *another translation*. Determine it explicitly.

#15.108 Let f_1 be rotation of the plane by an angle θ_1 , let f_2 be translation of the plane by vector v_2 , and let f_3 be rotation of the plane by an angle θ_3 . Show that

$$f_3 \circ f_2 \circ f_1$$

is expressible more briefly as $F \circ G$ where F is translation by some vector, and G is rotation by some angle.

#15.109 Let f_1 be translation of the plane by a vector v_1 , let f_2 be rotation of the plane by angle θ_2 , and let f_3 be translation of the plane by a vector v_3 . Show that

$$f_3 \circ f_2 \circ f_1$$

is expressible more briefly as $F \circ G$ where F is translation by some vector, and G is rotation by some angle.

#15.110 Let $R_\theta^{(z)}$ be a rotation around the z -axis by angle θ , $R_\theta^{(y)}$ a rotation around the y -axis by angle θ . Show that, given any vector $v = (x, y, z)$ with $\|v\| = 1$ there are angles α, β so that

$$R_\alpha^{(z)} \circ R_\beta^{(y)}(1, 0, 0) = (x, y, z)$$

#15.111 (*) Prove the assertion that left multiplication by the matrix

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

really does rotate points in the plane by the angle θ around the origin.

#15.112 (*) Let $R_\theta^{(z)}$ be rotation around the z -axis by θ , $R_\theta^{(y)}$ rotation around the y -axis by θ , and $R_\theta^{(x)}$ rotation around the x -axis by θ . Given two vectors v, w so that $\|v\| = \|w\| = 1$ and $\langle v, w \rangle = 0$, find angles α, β, γ so that

$$R_\alpha^{(x)} \circ R_\beta^{(y)} \circ R_\gamma^{(z)}(1, 0, 0) = v$$

$$R_\alpha^{(x)} \circ R_\beta^{(y)} \circ R_\gamma^{(z)}(0, 1, 0) = w$$

#15.113 (*) Let $R_\theta^{(z)}$ be rotation around the z -axis by θ , $R_\theta^{(y)}$ rotation around the y -axis by θ , and $R_\theta^{(x)}$ rotation around the x -axis by θ . For given θ_1, θ_2 , find α, β, γ so that

$$R_{\theta_1}^{(z)} \circ R_{\theta_2}^{(y)} = R_\alpha^{(x)} \circ R_\beta^{(y)} \circ R_\gamma^{(z)}$$

16. Permutations and Symmetric Groups

Another important fundamental idea is that of **permutation of a set** X . A permutation of a set is defined to be a bijection of X to itself.

The crudest question we can ask about permutations of X is *how many are there?* If X has n (distinct) elements x_1, x_2, \dots, x_n and $f : X \rightarrow X$ is a permutation of X , then there are n choices for what $f(x_1)$ can be, $n-1$ remaining choices for what $f(x_2)$ can be (since it can't be whatever $f(x_1)$ was, and so on. Thus, there are $n!$ permutations of a set with n elements.

To study permutations themselves it doesn't matter much exactly what the elements of the set are so long as we can tell them apart, so let's just look at the set

$$\{1, 2, 3, \dots, n-1, n\}$$

as a good prototype of a set with n (distinct elements). The standard notation is to write S_n for the **group of permutations** of n things. This S_n is also called the **symmetric group** on n things.

Despite the name 'symmetric group', these groups are not directly related to 'groups of symmetries' of geometric objects. At the same time, it can happen that a group of symmetries turns out to be a symmetric group. The point is that the terminology is a little delicate here, so be careful).

A standard way to write permutations f of $\{1, 2, \dots, n\}$ in order to describe in detail what f does is to effectively *graph* f but in the form of a list: write

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}$$

Thus, altering the notation just slightly, the permutation

$$g = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$$

is the one so that $g(i) = i_i$.

Always we have the **trivial permutation**

$$e = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

which does not 'move' any element of the set. That is, for all i , $e(i) = i$.

Of course, one permutation may be applied after another. If g, h are two permutations, write

$$g \circ h$$

for the permutation that we get by first applying h , and then applying g . This is the **composition** or **product** of the two permutations. It is important to appreciate that, *in general*

$$g \circ h \neq h \circ g$$

We'll see examples of this below. But in any case this notation is indeed compatible with the notation for (and the idea of) *composition of functions*. Thus, for $1 \leq i \leq n$, *by definition*

$$(g \circ h)(i) = g(h(i))$$

It is a consequence of the definition of permutations as (bijective) *functions* from a set to itself that *composition of permutations is associative*: for all permutations g, h, k of a set,

$$(g \circ h) \circ k = g \circ (h \circ k)$$

Indeed, for any element x of the set, the definition of composition of permutations gives

$$\begin{aligned} ((g \circ h) \circ k)(x) &= (g \circ h)(k(x)) && \text{definition of } (g \circ h) \circ k, \text{ applied to } x \\ &= g(h(k(x))) && \text{definition of } g \circ h, \text{ applied to } k(x) \\ &= g((h \circ k)(x)) && \text{definition of } h \circ k, \text{ applied to } x \\ &= (g \circ (h \circ k))(x) && \text{definition of } g \circ (h \circ k), \text{ applied to } x \end{aligned}$$

(This even works for infinite sets).

And for any permutation g there is the **inverse** permutation g^{-1} which has the effect of reversing the permutation performed by g . That is,

$$g \circ g^{-1} = g^{-1} \circ g = e$$

Often the little circle indicating composition is suppressed, and we just write

$$g \circ h = gh$$

as if it were ordinary multiplication. The hazard is that we cannot presume that $gh = hg$, so a little care is required.

The graph-list notation for permutations is reasonably effective in computing the *product* of two permutations: to compute, for example,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

we see what this composite does to each of 1, 2, 3. The permutation on the right is applied first. It sends 1 to 3, which is sent to 1 by the second permutation (the one on the left). Similarly, 2 is sent to 2 (by the permutation on the right) which is sent to 3 (by the permutation on the left). Similarly, 3 is sent to 1 (by the permutation on the right) which is sent to 2 (by the permutation on the left). Listing-graphing this information, we have

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

If we multiply (compose) in the opposite order, we get something different:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

This is the simplest example of the **non-commutativity** of the ‘multiplication’ of permutations, that is, that $gh \neq hg$ in general.

It is certainly true that permutations, especially of big sets, can be very complicated things which are hard to visualize. Still, they can be broken up into simple pieces, as we’ll see just below.

First, the simplest permutations are the **cycles** of various lengths. A **k -cycle** is a permutation f so that (for some numbers i_1, \dots, i_k)

$$f(i_1) = i_2, \quad f(i_2) = i_3, \quad f(i_3) = i_4, \dots, \quad f(i_{k-1}) = i_k, \quad f(i_k) = i_1$$

and so that $f(j) = j$ for any number j not in the list i_1, \dots, i_k . Note that i_k is sent back to i_1 . Thus, as the name suggests, f *cycles* the i_1, \dots, i_k among themselves. A more abbreviated notation is used for this: write

$$(i_1 \ i_2 \ \dots \ i_{k-1} \ i_k)$$

for this k -cycle.

For example, comparing with the more general notation,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1 \ 2)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 \ 3)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \ 2 \ 3)$$

These are, in order, two 2-cycles and a 3-cycle.

Unlike the more general notation, there is some *ambiguity* in the cycle notation: for example,

$$(1 \ 2 \ 3) = (2 \ 3 \ 1) = (3 \ 1 \ 2)$$

Generally, there are k different ways to write a k -cycle in this cycle notation. In a similar vein, it is pretty clear that

- If g is a k -cycle, then

$$g^k = e$$

meaning that applying g to the set k times has the net effect of *moving nothing*.

How do cycles interact with each other? Well, generally not very well, but if $g = (i_1 \dots i_k)$ and $h = (j_1 \dots j_\ell)$ are a k -cycle and an ℓ -cycle with *disjoint* lists $\{i_1, \dots, i_k\}$ and $\{j_1, \dots, j_\ell\}$ interact nicely: *they commute with each other*, meaning that

$$gh = hg$$

in this special scenario. Such cycles are called (reasonably enough) **disjoint cycles**. Pursuing this idea, we have

- Any permutation can be written as a product of disjoint cycles, and in essentially just one way.

The ‘essentially’ means that writing the same cycles in a different order is not to be considered different, since after all they *commute*. This is called a **decomposition into disjoint cycles**.

Knowing the decomposition into disjoint cycles of a permutation g is the closest we can come to understanding the nature of g . Happily, this decomposition can be determined in a systematic way (effectively giving an explicit proof of this assertion). For example, consider

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 5 & 7 & 6 & 1 \end{pmatrix}$$

We just trace the ‘path’ of elements under repeated applications of g . To start, let’s see what happens to 1 under repeated application of g : first 1 goes to 4, which then goes to 5, which then goes to 7, which then goes to 1. Since we have returned to 1, we have *completed the cycle*: we see that one cycle occurring inside g is

$$(1 \ 4 \ 5 \ 7)$$

Next, look at any number which didn't already occur in this cycle, for example 2. First 2 goes to 3, which then goes to 2, which already completes another cycle. Thus, there is also the 2-cycle

$$(2\ 3)$$

inside g . The only number which hasn't yet appeared in either of these cycles is 6, which is not moved by g . Thus, we have obtained the *decomposition into disjoint cycles*:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 5 & 7 & 6 & 1 \end{pmatrix} = (1\ 4\ 5\ 7)(2\ 3) = (2\ 3)(1\ 4\ 5\ 7)$$

And the decomposition into disjoint cycles tells how many times a permutation must be repeated in order to have no net effect: *the least common multiple of the lengths of the disjoint cycles appearing in its decomposition*.

The **order** of a permutation is the number of times it must be applied in order to have *no net effect*. (Yes, there is possibility of confusion with other uses of the word 'order'). Thus,

- The order of a k -cycle is k . The order of a product of disjoint cycles is the least common multiple of the lengths.

We might imagine that permutations with larger orders '*mix better*' than permutations with smaller orders, since more repetitions are necessary before the mixing effect is 'cancelled'. In this context, it may be amusing to realize that if a card shuffle is done perfectly, then after *some* number of repetitions the cards will be returned to their original order! But the number is pretty large with a 52-card deck, and it's not easy to do perfect shuffles anyway.

As an example, let's examine the all elements of S_7 , determining their structure as products of disjoint cycles, counting the number of each kind, and noting their order.

First, let's count the 7-cycles ($i_1 \dots i_7$): there are 7 choices for i_1 , 6 for i_2 , and so on, but there are 7 different ways to *write* each 7-cycle, so there are $7!/7$ distinct 7-cycles altogether.

Next, 6-cycles ($i_1 \dots i_6$): there are 7 choices for i_1 , 6 for i_2 , and so on down to 2 choices for i_6 , but there are 6 different ways to *write* each 6-cycle, so there are $7!/6$ distinct 6-cycles altogether.

Next, 5-cycles ($i_1 \dots i_5$): there are 7 choices for i_1 , 6 for i_2 , and so on down to 3 choices for i_5 , but there are 5 different ways to *write* each 5-cycle, so there are $7!/2!5$ distinct 5-cycles altogether.

For variety, let's count the number of permutations writeable as a product of disjoint 5-cycle and 2-cycle. We just counted that there are $7!/2!5$ distinct 5-cycles. But each choice of 5-cycle leaves just one choice for 2-cycle disjoint from it, so there are again $7!/2!5$ distinct products of disjoint 5-cycle and 2-cycle. And we note that the *order* of a product of disjoint 5 and 2-cycle is $lcm(2, 5) = 10$.

There are $7!/3!4$ distinct 4-cycles, by reasoning similar to previous examples.

There are $7!/3!4 \cdot 3!/2$ choices of disjoint 4-cycle and 2-cycle. The order of the product of such is $lcm(2, 4) = 4$.

There are $7!/3!4 \cdot 3!/3$ choices of disjoint 4-cycle and 3-cycle. The order of the product of such is $lcm(3, 4) = 12$.

There are $7!/4!3$ distinct 3-cycles, by reasoning similar to previous examples.

There are $7!/4!3 \cdot 4!/2!2$ choices of disjoint 3-cycle and 2-cycle. The order of the product of such is $lcm(2, 3) = 6$.

The number of disjoint 3-cycle, 2-cycle, and 2-cycle is slightly subtler, since *the two 2-cycles are indistinguishable*. Thus, there are

$$\frac{7!}{4!3} \frac{4!}{2!2} \frac{2!}{0!2} \cdot \frac{1}{2!}$$

where the last division by $2!$ is to take into account the $2!$ different orderings of the two 2-cycles, which make only a *notational* difference, *not* a difference in the permutation itself. The order of such a permutation is $\text{lcm}(2, 2, 3) = 6$.

The number of disjoint pairs of 3-cycle and 3-cycle is similar: the two 3-cycles are not actually ordered although our “choosing” of them gives the appearance that they are ordered. There are

$$\frac{7!}{4!3} \frac{4!}{1!3} \cdot \frac{1}{2!}$$

such pairs, where the last division by $2!$ is to take into account the $2!$ different orderings of the two 3-cycles, which make only a *notational* difference, *not* a difference in the permutation itself. The order of such a permutation is $\text{lcm}(3, 3, 1) = 3$.

There are $7!/5!2$ distinct 2-cycles, each of order 2.

There are $7!/5!2 \cdot 5!/3!2 \cdot 1/2!$ pairs of disjoint 2-cycles, where the last division by $2!$ is to take into account the possible orderings of the two 2-cycles, which affect the notation but not the permutation itself.

Finally, there are

$$\frac{7!}{5!2} \frac{5!}{3!2} \frac{3!}{1!2} \cdot \frac{1}{3!}$$

triples of disjoint 2-cycles, where the last division by $3!$ is to account for the possible orderings of the 3 2-cycles, which affects the notation but not the permutation itself. The order of such a permutation is just $\text{lcm}(2, 2, 2) = 2$.

As a by-product of this discussion, we see that the largest order of any permutation of 7 things is 12, which is obtained by taking the product of disjoint 3 and 4-cycles.

As a more extreme example of the counting issues involved, let’s count the disjoint products of three 2-cycles and three 5-cycles in S_{24} . As above, this is

$$\frac{24!}{22!2} \frac{22!}{20!2} \frac{20!}{18!2} \frac{1}{3!} \cdot \frac{18!}{13!5} \frac{13!}{8!5} \frac{8!}{3!5} \frac{1}{3!}$$

where both of the divisions by $3!$ come from discounting the possible orderings of the 2-cycles, and the possible orderings of the 5-cycles. Note that since 2-cycles are distinguishable from 5-cycles, there is no further accounting necessary for the ordering of the 2-cycles *relative to the 5-cycles*, etc.

And we can break down any permutation into a *product of 2-cycles* (likely *not* disjoint). The procedure to do this is as follows. First, write the permutation as a product of *cycles*. This reduces the problem to that of writing any *cycle* as a product of 2-cycles. It’s not hard to check that

$$(i_1 i_2 \dots i_k) = (i_1 i_2)(i_2 i_3) \dots (i_{k-1} i_k)$$

That is, a k -cycle is a (certainly *not* disjoint) product of $k - 1$ two-cycles.

- Let f be a permutation. The number n of 2-cycles needed to express f as a product of n two-cycles is not uniquely determined, but n modulo 2 is uniquely determined.

A permutation written as a product of an *odd* number of 2-cycles is an **odd permutation**, while a permutation written as a product of an *even* number of two-cycles is an **even permutation**.

The collection A_n of all *even* permutations in the symmetric group S_n is the **alternating group** on n things. *The composition of two even permutations is again even.*

#16.114 Express The following as products of disjoint cycles, as products of two-cycles, and determine their order.

$$\begin{aligned} & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 4 & 7 & 1 & 3 & 6 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 7 & 1 & 5 & 6 \end{pmatrix} \end{aligned}$$

#16.115 Compute the product

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 4 & 7 & 1 & 3 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 7 & 1 & 5 & 6 \end{pmatrix}$$

#16.116 How many distinct 3-cycles are there in S_5 ? (*Hint:* In cycle notation, a 3 cycle is specified by a notation using 3 distinct elements of the set being permuted. And now order really does matter. *But* there is a *little* redundancy: there are still k different ways to write the same k -cycle.)

#16.117 Count the number of elements of S_4 of each possible order, by identifying them as products of disjoint cycles of various orders.

#16.118 Count the number of elements of A_5 of all possible orders, by identifying them as products of disjoint cycles of various orders, and excluding those which are *odd* permutations.

#16.119 For any $g, h \in S_n$, show that the *commutator* $ghg^{-1}h^{-1}$ is an *even* permutation.

17. Groups: Lagrange's Theorem, Euler's Theorem

Here we encounter the first instance of *abstract algebra* rather than the *tangible algebra* studied in high school.

One way to think of the point of this is that it is an attempt to study the *structure* of things directly, without reference to irrelevant particular details.

This also achieves amazing efficiency (in the long run, anyway), since it turns out that the same underlying structures occur over and over again in mathematics. Thus, a careful study of these basic structures is amply repaid by allowing a much simpler and more unified mental picture of otherwise seemingly-different phenomena.

- Groups
- Subgroups
- Lagrange's theorem
- Index of a subgroup
- Laws of Exponents
- Cyclic subgroups, orders, exponents
- Euler's theorem
- Exponents of groups

17.1 Groups

The simplest (but maybe not most immediately intuitive) object in abstract algebra is a *group*. This idea is pervasive in modern mathematics. Many seemingly elementary issues seem to be merely secret manifestations of facts about groups. This is especially true in elementary number theory, where it is *possible* to give “elementary” proofs of many results, but only at the cost of having everything be complicated and so messy that it can't be remembered.

A **group** G is a set with an operation $g * h$, with a special element e called **the identity**, and with properties:

- The property of the identity: for all $g \in G$, $e * g = g * e = g$.
- Existence of **inverses**: for all $g \in G$ there is $h \in G$ (the **inverse** of g) so that $h * g = g * h = e$.
- Associativity: for all $x, y, z \in G$, $x * (y * z) = (x * y) * z$.

If the operation $g * h$ is *commutative*, that is, if

$$g * h = h * g$$

then the group is said to be **abelian** (named after N.H. Abel, born on my birthday but 150 years earlier). In that case, often, but not always, the operation is written as *addition*. And if the operation is written as addition, then the identity is often written as 0 instead of e .

And in many cases the group operation is written as multiplication

$$g * h = g \cdot h = gh$$

This does not *preclude* the operation being abelian, but rather suggests only that there is no *presumption* that the operation is abelian. If the group operation is written as multiplication, then often the identity is written as 1 rather than e . Especially when the operation is written simply as *multiplication*, the **inverse** of an element g in the group is written as

$$\text{inverse of } g = g^{-1}$$

If the group operation is written as *addition*, then the inverse is written as

$$\text{inverse of } g = -g$$

In each of the following examples, it is easy to verify the properties necessary for the things to qualify as *groups*: we need an *identity* and we need *inverses*, not to mention *associativity*.

- The integers \mathbf{Z} with operation the usual addition $+$. The identity is 0 and the inverse of x is $-x$. This group is *abelian*.
- The *even* integers $2\mathbf{Z}$ with the usual addition $+$. The identity is 0 and the inverse of x is $-x$. This group is *abelian*.
- The set $7\mathbf{Z}$ of multiples of 7 among integers, with the usual addition $+$. The identity is 0 and the inverse of x is $-x$. This group is *abelian*.
- The set \mathbf{Z}/m of integers-mod- m , with addition-mod- m as the operation. The identity is 0-mod- m and the inverse of x -mod- m is $(-x)$ -mod- m . This group is *abelian*.
- The set \mathbf{Z}/m^\times of integers mod m *relatively prime to* m , with multiplication-mod- m as the operation. The identity is 1-mod- m . In this example, a person unacquainted with arithmetic mod m would not realize that *there are multiplicative inverses*. We can compute them via the Euclidean algorithm. So this is the first ‘non-trivial’ example. This group is *abelian*.
- The collection of vectors in real n -space \mathbf{R}^n , with operation vector addition. The identity is just the 0 vector. Inverses are just negatives. (Note that we are literally *forgetting* the fact that there is a scalar multiplication).
- The set $GL(2, \mathbf{R})$ of invertible two-by-two real matrices, with group law matrix multiplication. Here the identity is the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The existence of inverses is just part of the definition. The fact that matrix multiplication is *associative* is not obvious from the definition, but this can either be checked by hand or inferred from ‘higher principles’. The fact that the product of two invertible matrices is invertible is interesting: suppose that g, h both have inverses, g^{-1} and h^{-1} , respectively. Then you can check that $h^{-1}g^{-1}$ is an inverse to gh . This group is certainly not abelian.

- Permutations of a set form a group, with operation being *composition* (as functions) of permutations. The do-nothing permutation is the identity. The associativity follows because permutations are *mappings*. If there are more than two things, these permutations groups are certainly non-abelian.

- The collection of all bijective functions from a set S to itself form a group, with the operation being composition of functions. The identity is the function e which maps every element just back to itself, that is, $e(s) = s$ for all $s \in S$. (This example is just a more general paraphrase of the previous one about permutations!)

17.2 Subgroups

Subgroups are subsets of groups which are groups “in their own right”.

A subset H of a group G is said to be a **subgroup** if, with the same operation as that used in G , it is a group.

That is, if H contains the identity element $e \in G$, if H contains inverses of all elements in it, and if H contains products of any two elements in it, then H is a subgroup. (The associativity of the operation is assured since the operation was *assumed* associative for G itself to be a group).

Another paraphrase: if $e \in H$, and if for all $h \in H$ the inverse h^{-1} is also in H , and if for all $h_1, h_2 \in H$ the product $h_1 h_2$ is again in H , then H is a subgroup of G .

Another cute paraphrase is: if $e \in H$, and if for all $h_1, h_2 \in H$ the product $h_1 h_2^{-1}$ is again in H , then H is a subgroup of G . (If we take $h_1 = e$, then the latter condition assures the existence of inverses! And so on).

In any case, one usually says that H is **closed under inverses** and **closed under the group operation**.

For example, the collection of all *even* integers is a subgroup of the additive group of integers. More generally, for fixed integer m , the collection H of all multiples of m is a subgroup of the additive group of integers. To check this: first, the identity 0 is a multiple of m , so $0 \in H$. And for any two integers x, y divisible by m , write $x = ma$ and $y = mb$ for some integers a, b . Then using the ‘cute’ paraphrase, we see that

$$x - y = ma - mb = m(a - b) \in H$$

so H is *closed under inverses and under the group operation*. Thus, it is a subgroup of \mathbf{Z} .

17.3 Lagrange’s Theorem

The theorem of this section is the simplest example of the use of group theory as *structured counting*. Although the discussion of this section is completely abstract, it gives the easiest route to (the very tangible) Euler’s theorem proven as a corollary below.

A **finite group** is simply a group which is also finite. The **order** of a finite group is the number of elements in it. Sometimes the order of a group G is written as $|G|$. Throughout this section we will write the group operation simply as though it were ordinary multiplication.

Theorem: (*Lagrange*) Let G be a *finite* group. Let H be a subgroup of G . Then the order of H *divides* the order of G .

For the proof we need some other ideas which themselves will be reused later. For subgroup H of a group G , and for $g \in G$, the **left coset** of H by g or **left translate** of H by g is

$$gH = \{gh : h \in H\}$$

The notation gH is simply shorthand for the right-hand side. Likewise, the **right coset** of H by g , or **right translate** of H by g is

$$Hg = \{hg : h \in H\}$$

Proof: First, we will prove that the collection of all left cosets of H is a *partition* of G , meaning that every element of G lies in *some* left coset of H , and if two left cosets xH and yH have non-empty intersection then actually $xH = yH$. (Note that this need not imply $x = y$.)

Certainly $x = x \cdot e \in xH$, so every element of G lies in a left coset of H .

Now suppose that $xH \cap yH \neq \phi$ for $x, y \in G$. Then for some $h_1, h_2 \in H$ we have $xh_1 = yh_2$. Multiply both sides of this equality on the right by h_2^{-1} to obtain

$$(xh_1)h_2^{-1} = (yh_2)h_2^{-1}$$

The right-hand side of this is

$$\begin{aligned} (yh_2)h_2^{-1} &= y(h_2h_2^{-1}) \quad (\text{by associativity}) \\ &= y \cdot e \quad (\text{by property of inverse}) \\ &= y \quad (\text{by property of } e) \end{aligned}$$

Let $z = h_1h_2^{-1}$ for brevity. By associativity in G ,

$$y = (xh_1)h_2^{-1} = x(h_1h_2^{-1}) = xz$$

Since H is a *subgroup*, $z \in H$.

Then

$$yH = \{yh : h \in H\} = \{(xz)h : h \in H\} = \{x(zh) : h \in H\}$$

On one hand, since H is closed under multiplication, for each $h \in H$ the product zh is in H . Therefore,

$$yH = \{x(zh) : h \in H\} \subset \{xh' : h' \in H\} = xH$$

Thus, $yH \subset xH$. But the relationship between x and y is completely symmetrical, so also $xH \subset yH$. Therefore $xH = yH$. (In other words, we have shown that the left cosets of H in G really do *partition* G .)

Next, we will show that the cardinalities of the left cosets of H are *all the same*. To do this, we show that there is a *bijection* from H to xH for any $x \in G$. In particular, define

$$f(g) = xg$$

(It is clear that this really does map H to yH .) Second, we prove *injectivity*: if $f(g) = f(g')$, then

$$xg = xg'$$

Left multiplying by x^{-1} gives

$$x^{-1}(xg) = x^{-1}(xg')$$

Using associativity gives

$$(x^{-1}x)g = (x^{-1}x)g'$$

Using the property $x^{-1}x = e$ of the inverse x^{-1} gives

$$eg = eg'$$

Since $eg = g$ and $eg' = g'$, by the defining property of the identity e , this is

$$g = g'$$

which is the desired injectivity. For *surjectivity*, we simply note that by its very definition the function f was arranged so that

$$f(h) = xh$$

Thus, any element in xH is hit by an element from H . Thus, we have the bijectivity of f , and all left cosets of H have the same number of elements as does H itself.

So G is the union of all the different left cosets of H (no two of which overlap). Let i be the number of different cosets of H . We just showed that every left coset of H has $|H|$ elements. Then we can count the number of elements in G as

$$|G| = \text{sum of cardinalities of cosets} = i \times |H|$$

Both sides of this equation are integers, so $|H|$ divides $|G|$, as claimed. ♣

17.4 Index of a subgroup

Having introduced the idea of a *coset* in the proof of Lagrange's theorem, we can now define the *index* of a subgroup.

Let G be a group, and H a subgroup of G . The **index** of H in G , denoted

$$[G : H]$$

is the number of (left) cosets of H in G .

Corollary: (of Lagrange's theorem) For a finite group G and subgroup H ,

$$|G| = [G : H] \cdot |H|$$

Proof: This is just a recapitulation of the counting done in proving Lagrange's theorem: we show that G is the disjoint union of the left cosets of H , and that each such coset has $|H|$ elements. Thus, the statement of this corollary is an assertion that counting the elements in G in two ways gives the same result. ♣

A closely related counting or divisibility principle is the following **multiplicative property** of indices of subgroups:

Proposition: Let G be a finite group, let H, I be subgroups of G , and suppose that $H \supset I$. Then

$$[G : I] = [G : H] \cdot [H : I]$$

Proof: The group G is a disjoint union of $[G : I]$ left cosets of I . Also, G is the disjoint union of $[G : H]$ left cosets of H . If we can show that any left *coset* of H is a disjoint union of $[H : I]$ left cosets of I , then the assertion of the proposition will follow.

Let

$$gH = \{gh : h \in H\}$$

be a left coset of H . And express H as a (disjoint) union of $[H : I]$ left cosets of I by

$$H = h_1I \cup h_2I \cup \dots \cup h_{[H:I]}I$$

Then

$$gH = g(h_1I \cup h_2I \cup \dots \cup h_{[H:I]}I) = gh_1I \cup gh_2I \cup \dots \cup gh_{[H:I]}I$$

which is certainly a union of left cosets of I . We might want to check that $h_iI \cap h_jI = \phi$ (for $i \neq j$) implies that

$$gh_iI \cap gh_jI = \phi$$

Suppose that $g \in gh_iI \cap gh_jI$. Then for some $i_1 \in I$ and $i_2 \in I$ we have

$$gh_i i_1 = x = gh_j i_2$$

Left multiplying by g^{-1} gives

$$h_i i_1 = h_j i_2$$

The left-hand side is (by hypothesis) an element of h_iI , and the right-hand side is an element of h_jI . But we had assumed that $h_iI \cap h_jI = \phi$, so this is impossible. That is, we have proven that $gh_iI \cap gh_jI = \phi$ if $h_iI \cap h_jI = \phi$. This certainly finishes the proof of the multiplicative property of subgroup indices. ♣

17.5 Laws of Exponents

It should be emphasized that the so-called *Laws of Exponents* are not “laws” at all, but are *provable properties* of the exponential notation. And the exponential notation itself is basically nothing more than an abbreviation for repeated multiplication.

Of course, we must be sure to be explicit about this *exponential notation* g^n for integer n , where g is an element of a group G . This is, after all, merely an abbreviation: first,

$$g^0 = e$$

and

$$g^n = \underbrace{g \cdot g \cdot \dots \cdot g}_n \quad (\text{for } n \geq 0)$$

$$g^n = \underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{|n|} \quad (\text{for } n \leq 0)$$

A more precise though perhaps less intuitive way of defining g^n is by **recursive definitions**:

$$g^n = \begin{cases} e & \text{for } n = 0 \\ g \cdot g^{n-1} & \text{for } n > 0 \\ g^{-1} \cdot g^{n+1} & \text{for } n < 0 \end{cases}$$

These are the definitions that lend themselves both to computation and to proving things.

While we’re here, maybe we should check that the so-called *Laws of Exponents* really do hold:

Proposition: (*Laws of Exponents*) For g in a group G , for integers m, n

- $g^{m+n} = g^m \cdot g^n$
- $g^{mn} = (g^m)^n$

Proof: The least obvious thing to prove is that

$$(g^{-1})^{-1} = g$$

Note that we absolutely cannot simply pretend to invoke “laws of exponents” to prove this! Instead, to prove this, we must realize that the way that one checks that y is an inverse of x is to compute xy and yx and see that they are both just e . So to prove that x is the inverse of x^{-1} , we must compute both $x^{-1}x$ and xx^{-1} . And, indeed, by the property of x^{-1} these both are e .

The rest of the proof is an exercise in *induction*, and is a bit tedious. And nothing really exciting happens.

Let’s prove that

$$g^{m+n} = g^m \cdot g^n$$

for m and n non-negative integers. We prove this by induction on n . For $n = 0$ the assertion is true, since

$$g^{m+0} = g^m = g^m \cdot e = g^m \cdot g^0$$

Then for $n > 0$,

$$g^{m+n} = g^{(m+n-1)+1} = g^{m+n-1} \cdot g$$

by the recursive definition of g^{m+n} . By induction,

$$g^{m+n-1} = g^m \cdot g^{n-1}$$

Therefore,

$$g^{m+n-1} \cdot g = (g^m \cdot g^{n-1}) \cdot g = g^m \cdot ((g^{n-1}) \cdot g)$$

by associativity. Now from the recursive definition of g^n we obtain

$$g^m \cdot ((g^{n-1}) \cdot g) = g^m \cdot g^n$$

This proves this “Law” for $m, n \geq 0$. ♣

17.6 Cyclic subgroups, orders, exponents

For an element g of a group G , let

$$\langle g \rangle = \{g^n : n \in \mathbf{Z}\}$$

This is called the **cyclic subgroup of G generated by g** .

The smallest positive integer n (if it exists!) so that

$$g^n = e$$

is the **order** or **exponent** of g . The order of a group element g is often denoted by $|g|$. Yes, we are reusing the terminology “order”, but it will turn out that these uses are compatible (just below).

Corollary: (*of Laws of Exponents*) For g in a group G , the subset $\langle g \rangle$ of G really is a subgroup of G .

Proof: The associativity is *inherited* from G . The *closure* under the group operation and the closure under taking inverses both follow immediately from the Laws of Exponents, as follows. First, the inverse of g^n is just g^{-n} , since

$$g^n \cdot g^{-n} = g^{n+(-n)} = g^0 = e$$

And closure under multiplication is

$$g^m \cdot g^n = g^{m+n}$$

♣

Theorem: Let g be an element of a finite group G . Let n be the order of g . Then the order of g (as group *element*) is equal to the order of $\langle g \rangle$ (as subgroup). Specifically,

$$\langle g \rangle = \{g^0, g^1, g^2, \dots, g^{n-1}\}$$

Generally, for arbitrary integers i, j ,

$$g^i = g^j \quad \text{if and only if} \quad i \equiv j \pmod{n}$$

Proof: The last assertion easily implies the first two, so we'll just prove the last assertion. On one hand, if $i \equiv j \pmod{n}$, then write $i = j + \ell m$ and compute (using Laws of Exponents):

$$g^i = g^{j+\ell m} = g^j \cdot (g^n)^\ell = g^j \cdot e^\ell = g^j \cdot e = g^j$$

On the other hand, suppose that $g^i = g^j$. Without loss of generality, exchanging the roles of i and j if necessary, we may suppose that $i \leq j$. Then $g^i = g^j$ implies $e = g^{j-i}$. Using the Reduction/Division algorithm, write

$$j - i = q \cdot n + r$$

where $0 \leq r < n$. Then

$$e = g^{j-i} = g^{qn+r} = (g^n)^q \cdot g^r = e^q \cdot g^r = e \cdot g^r = g^r$$

Therefore, since n is the least positive integer so that $g^n = e$, it must be that $r = 0$. That is, $n|j - i$, which is to say that $i \equiv j \pmod{n}$ as claimed. ♣

Corollary: (*of Lagrange's theorem*) The order $|g|$ of an element g of a finite group G divides the order of G .

Proof: We just proved that $|g| = |\langle g \rangle|$. By Lagrange's theorem, $|\langle g \rangle|$ divides $|G|$, which yields this corollary. ♣

17.7 Euler's Theorem

Now we return to number theory, and give a clean and conceptual proof of Euler's identity, as a corollary of Lagrange's theorem and the discussion of Laws of Exponents and cyclic subgroups. Further, we can give a slightly refined form of it.

Let $\varphi(n)$ be Euler's phi-function, counting the number of integers ℓ in the range $0 < \ell \leq n$ which are relatively prime to n . The proof we give of this is simply the abstracted version of Euler's original argument.

Theorem: Let n be a positive integer. For $x \in \mathbf{Z}$ relatively prime to n ,

$$x^{\varphi(n)} \equiv 1 \pmod{n}$$

Proof: The set \mathbf{Z}/n^\times of integers-mod- n which are relatively prime to n has $\varphi(n)$ elements. By Lagrange's theorem and its corollaries just above, this implies that the order k of $g \in \mathbf{Z}/n^\times$ divides $\varphi(n)$. Therefore, $\varphi(n)/k$ is an integer, and

$$g^{\varphi(n)} = (g^k)^{\varphi(n)/k} = e^{\varphi(n)/k} = e$$

Applied to $x \pmod{n}$ this is the desired result. ♣

Remark: This approach also gives another proof of Fermat's theorem, dealing with the case that n is prime, without mention of binomial coefficients.

Further, keeping track of what went into the proof of Euler's theorem in the first place, we have

Theorem: Let n be a positive integer. For $x \in \mathbf{Z}$ relatively prime to n , the smallest exponent ℓ so that

$$x^\ell \equiv 1 \pmod{n}$$

is a divisor of $\varphi(n)$. That is, the order of x in the multiplicative group \mathbf{Z}/n^\times is a divisor of $\varphi(n)$.

Proof: The proof is really the same: the order of x is equal to the order of the subgroup $\langle x \rangle$, which by Lagrange's theorem is a divisor of the order of the whole group \mathbf{Z}/n^\times . ♣

17.8 Exponents of groups

The idea of Euler's theorem can be made more precise and abstracted.

For a group G , the smallest positive integer ℓ so that for every $g \in G$

$$g^\ell = e$$

is the **exponent** of the group G . It is not clear from the definition that there really is such a positive integer ℓ . Indeed, for *infinite* groups G there may not be. But for *finite* groups the mere finiteness allows us to characterize the exponent:

Proposition: Let G be a finite group. Then the exponent of G exists, and in particular

$$\text{exponent of } G = \text{least common multiple of } |g| \text{ for } g \in G$$

Proof: If $g^k = e$, then we know from discussion of cyclic subgroups above that $|g|$ divides k . And, on the other hand, if $k = m \cdot |g|$ then

$$g^k = g^{m \cdot |g|} = (g^{|g|})^m = e^m = e$$

Since G is finite, every element of it is of finite order. And, since there are only finitely-many elements in G , the least common multiple M of their orders exists. From what we've just seen, surely $g^M = e$ for any g . Thus, G does have an exponent. And if $g^k = e$ for all $g \in G$ then k is divisible by the orders of all elements of G , so by their least common multiple. Thus, the exponent of G really is the least common multiple of the orders of its elements. ♣

And Lagrange's theorem gives a limitation on what we can expect the exponent to be:

Corollary: (of Lagrange's theorem) Let G be a finite group. Then the exponent of G divides the order $|G|$ of G .

Proof: From the proposition, the exponent is the least common multiple of the orders of the elements of G . From Lagrange's theorem, each such order is a divisor of $|G|$. The least common multiple of any collection of divisors of a fixed number is certainly a divisor of that number. ♣

#17.120 Prove that in any group G for any elements $h, x, y \in G$ we have

$$h(xy)h^{-1} = (h x h^{-1})(h y h^{-1})$$

#17.121 Prove (by induction) that in any group G for any elements $g, h \in G$ and for any integer n

$$h g^n h^{-1} = (h g h^{-1})^n$$

#17.122 Make an addition table for $\mathbf{Z}/4$ and a multiplication table for $\mathbf{Z}/5^\times$.

#17.123 Why isn't $\{1, 2, 3, 4, 5\}$ with operation *multiplication modulo 6* a group?

#17.124 Prove by induction that in an *abelian* group G we have

$$(gh)^n = g^n h^n$$

for all $g, h \in G$, and for all positive integers n .

#17.125 Show that

$$(gh)^2 = g^2 h^2$$

in a group if and only if $gh = hg$.

#17.126 Prove that $(gh)^{-1} = h^{-1} g^{-1}$.

#17.127 Prove that $(gh)^{-1} = g^{-1} h^{-1}$ if and only if $gh = hg$.

#17.128 Prove that the intersection $H \cap K$ of two subgroups H, K of a group G is again a subgroup of G .

#17.129 Show that in an *abelian* group G , for a fixed positive integer n the set X_n of elements g of G so that $g^n = e$ is a subgroup of G .

#17.130 There are 8 subgroups of the group $\mathbf{Z}/30^\times$. Find them all. (List each subgroup only once!)

#17.131 Check that the collection of matrices g in $GL(2, \mathbf{Q})$ of the form $g = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ (that is, with lower left and upper right entries 0) is a *subgroup* of $GL(2, \mathbf{Q})$.

#17.132 Check that the collection of matrices g in $GL(2, \mathbf{Q})$ of the form $g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ (that is, with lower left entry 0) is a *subgroup* of $GL(2, \mathbf{Q})$.

#17.133 (*Casting out nines:*) Show that

$$123456789123456789 + 234567891234567891$$

$$\neq 358025680358025680$$

(*Hint*: Look at things modulo 9: if two things are not equal mod 9 then they certainly aren't equal. And notice the funny general fact that, for example,

$$1345823416 \equiv 1 + 3 + 4 + 5 + 8 + 2 + 3 + 4 + 1 + 6 \pmod{9}$$

since $10 \equiv 1 \pmod{9}$, and $100 \equiv 1 \pmod{9}$, and so on. The assertion is that a decimal number is congruent to the sum of its digits modulo 9! This is *casting out nines*, which allows detection of some errors in arithmetic).

#17.134 By casting out 9's, show that

$$\begin{aligned} &123456789123456789 \times 234567891234567891 \\ &\neq 28958998683279996179682996625361999 \end{aligned}$$

Certainly in *this* case it's not possible to check *directly* by hand, and probably most calculators would overflow.

#17.135 Prove that a group element and its inverse have the same order.

#17.136 Without computing, show that in the group $\mathbf{Z}/100$ (with addition) the elements 1, 99 have the same order, as do 11, 89.

#17.137 Find the orders of the following elements g, h of $GL(2, \mathbf{R})$:

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

Compute the product gh , compute $(gh)^n$ for integers n , and then show that gh is necessarily of *infinite order* in the group.

#17.138 Let G be a finite group. Let N be the *least common multiple* of the orders of the elements of G . Show that for all $g \in G$ we have $g^N = e$.

#17.139 (*) Let G be an *abelian* group. Let m, n be relatively prime positive integers. Let g be an element of order m and let h be an element of order n . Show that $|gh| = mn$. More generally, show that without any relative primeness hypothesis on the orders of g, h show that $|gh|$ is the *least common multiple* of $|g|, |h|$.

#17.140 Let x be an element of a group G and suppose that $x^{3 \cdot 5} = e$ and $x^3 \neq e$. Show that the order of x is either 5 or 15.

#17.141 Show that any integer i so that $1 \leq i < 11$ is a generator for the additive group $\mathbf{Z}/11$ of integers modulo 11.

#17.142 Check that $\mathbf{Z}/8^\times$ cannot be generated by a single element.

#17.143 Find all 5 of the distinct subgroups of the group $\mathbf{Z}/16$ (with addition). (List each subgroup only once!)

#17.144 Prove that if an element g of a group G has order n and if d is a divisor of n then $g^{n/d}$ has order d . (Equivalently, g^d has order n/d).

18. Rings and Fields: definitions and first examples

- Rings, fields
 - Divisibility in rings
 - Polynomial rings
 - Euclidean algorithm in polynomial rings
 - Euclidean rings
-

18.1 Rings, fields

The idea of **ring** generalizes the idea of ‘numbers’, among other things, so maybe is a little more intuitive than the idea of **group**.

A **ring** R is a set with two operations, $+$ and \cdot , and with a special element 0 (**additive identity**) with most of the usual properties we expect or demand of ‘addition’ and ‘multiplication’:

- The addition is **associative**: $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$.
- The addition is **commutative**: $a + b = b + a$ for all $a, b \in R$.
- For every $a \in R$ there is an **additive inverse** denoted $-a$, with the property that $r + (-r) = 0$.
- The zero has the property that $0 + a = a + 0 = a$ for all $a \in R$.
- The multiplication is **associative**: $a(bc) = (ab)c$ for all $a, b, c \in R$.
- The multiplication and addition have left and right **distributive** properties: $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b \in R$.

When we write this multiplication, just as in high school algebra, very often the dot will be omitted, and just write

$$ab = a \cdot b$$

Very often, a particular ring has some additional special features or properties:

- If there is an element 1 in a ring with the property that $1 \cdot a = a \cdot 1$ for all $a \in R$, then 1 is said to be **the (multiplicative) identity** or **unit** in the ring, and the ring is said to **have an identity** or **have a unit** or be a **ring with unit**. And 1 is **the unit** in the ring. We also demand that $1 \neq 0$ in a ring.
- If $ab = ba$ for all a, b in a ring R , that is, if multiplication is **commutative**, then the ring is said to be a **commutative ring**.

Most often, but not always, our rings of interest will have units ‘1’. The condition of commutativity of multiplication is often met, but, for example, *matrix multiplication is not commutative*.

- In a ring R with 1 , for a given element $a \in R$, if there is $a^{-1} \in R$ so that $a \cdot a^{-1} = a^{-1} \cdot a$, then a^{-1} is said to be a **multiplicative inverse** for a . If $a \in R$ has a multiplicative inverse, then a is called a **unit** in R . The collection of all units in a ring R is denoted R^\times , and is called **the group of units in R** .

- A commutative ring in which every non-zero element is a *unit* is called a **field**.
- A not-necessarily commutative ring in which every non-zero element is a unit is called a **division ring**.
- In a ring R an element r so that $r \cdot s = 0$ or $s \cdot r = 0$ for some non-zero $s \in R$ is called a **zero divisor**. A commutative ring *without* non-zero zero-divisors is an **integral domain**.
- A commutative ring R has the **cancellation property** if for any $r \neq 0$ in R if $rx = ry$ for $x, y \in R$ then $x = y$. Most rings with which we're familiar have this property.

Comment on terminology: There is indeed an inconsistency in the use of the word *unit*. But that's the way the word is used. So *the* unit is 1, while *a* unit is merely something which has a multiplicative inverse. Of course, there are *no* multiplicative inverses unless there is a unit (meaning that there is a 1!). *It is almost always possible to tell from context what is meant.*

It is very important to realize that the notation $-a$ for an additive inverse and a^{-1} for multiplicative inverse are meant to *suggest* 'minus a ' and 'divide-by- a ', but that at the moment we are *not justified* in believing any of the 'usual' high school algebra properties. *We have to prove that all the 'usual' things really do still work in this abstract situation.*

If we take a ring R with 0 and with its addition, then we get an abelian group, called **the additive group of R** .

The group of units R^\times in a ring with unit certainly is a group. Its identity is the unit 1. This group is abelian if R is commutative.

In somewhat more practical terms: as our examples above show, very often a *group* really is just the *additive group* of a ring, or is the *group of units* in a ring. There are many examples where this is not really so, but many fundamental examples are of this nature.

The integers \mathbf{Z} with usual addition and multiplication form a ring. This ring is certainly *commutative* and has a multiplicative identity '1'. The group of units \mathbf{Z}^\times is just $\{\pm 1\}$. This ring is an integral domain.

The *even* integers $2\mathbf{Z}$ with the usual addition and multiplication form a commutative ring *without* unit. Just as this example suggests, very often the lack of a unit in a ring is somewhat artificial, because there is a 'larger' ring it sits inside which *does* have a unit. There are no units in this ring.

The 'integers mod m ' \mathbf{Z}/m form a commutative ring with identity. *As the notation suggests*, the group of units really is \mathbf{Z}/m^\times : notice that we used the group-of-units notation in this case before we even introduced the terminology.

Take p a prime. The ring of integers mod p \mathbf{Z}/p is a *field* if p is *prime*, since all positive integers less than p have a multiplicative inverse modulo p for p prime (computable by the Euclidean Algorithm!). The group of units really is \mathbf{Z}/p^\times .

The collection of n -by- n real matrices (for fixed n) is a ring, with the usual matrix addition and multiplication. Except for the silly case $n = 1$, this ring is *non-commutative*. The group of units is the group $GL(n, \mathbf{R})$.

The rational numbers \mathbf{Q} , the real numbers \mathbf{R} , and the complex numbers \mathbf{C} are all examples of *fields*, because all their non-zero elements have multiplicative inverses.

Let p be a prime number. Then \mathbf{Z}/p with addition and multiplication modulo p is a *field*, because (by use of the Euclidean algorithm, for example) any $x \not\equiv 0 \pmod{p}$ has a multiplicative inverse modulo p .

Just as in the beginning of our discussion of *groups*, there are some things which we might accidentally take for granted about how rings behave, and reasonably so, after all, based on all our previous experience with numbers, etc. But it is certainly better to give the 'easy' little proofs of these things and to be conscious of what we believe, rather than to be unconscious.

Let R be a ring. We will prove the following fundamental properties:

- *Uniqueness of additive identity:* If there is an element $z \in R$ and another $r \in R$ so that $r + z = r$, then $z = 0$. (Note that we only need this condition for *one* other $r \in R$, not for *all* $r \in R$).
- *Uniqueness of additive inverses:* Fix $r \in R$. If there is $r' \in R$ so that $r + r' = 0$, then actually $r' = -r$, the additive inverse of r .
- *Uniqueness of multiplicative identity:* Suppose that R has a unit 1 . If there is $u \in R$ so that for all $r \in R$ we have $u \cdot r = r$, then $u = 1$. Or, if for all $r \in R$ we have $r \cdot u = r$, then $u = 1$. Actually, all we need is that *either* $1 \cdot u = 1$ *or* $u \cdot 1 = 1$ to assure that $u = 1$.
- *Uniqueness of multiplicative inverses:* If $r \in R$ has a multiplicative inverse r^{-1} , and if $r' \in R$ is such that $r \cdot r' = 1$, then $r' = r^{-1}$. Or, assuming instead that $r' \cdot r = 1$, we still conclude that $r' = r^{-1}$.
- For $r \in R$, we have $-(-r) = r$. That is, the additive inverse of the additive inverse of r is just r .

Proof of uniqueness of additive identity: If there is an element $z \in R$ and $r \in R$ so that $r + z = r$, add $-r$ to both sides of this equation to obtain

$$(r + z) - r = r - r = 0$$

by definition of additive inverse. Using the commutativity and associativity of addition, the left-hand side of this is

$$(r + z) - r = (z + r) - r = z + (r - r) = z + 0 = z$$

also using the property of the 0. That is, putting this together, $z = 0$, proving what we wanted.

Proof of uniqueness of additive inverses: Fix $r \in R$. If there is $r' \in R$ so that $r + r' = 0$, then add $-r$ to both sides to obtain

$$(r + r') - r = 0 + (-r)$$

Using the commutativity and associativity of addition, the left-hand side of this is

$$(r + r') - r = (r' + r) - r = r' + (r - r) = r' + 0 = r'$$

Since the right hand side is $0 + (-r) = -r$, we have $r' = -r$, as claimed.

Proof of uniqueness of multiplicative identity: Suppose that *either* $1 \cdot u = 1$ *or* $u \cdot 1 = 1$ to assure that $u = 1$. Well, let's just do one case, since the other is identical apart from writing things in the opposite order. Suppose that $u \cdot 1 = 1$. Then since $u \cdot 1 = u$ by the property of the multiplicative identity 1, we have $u = 1$. Done.

Proof of uniqueness of multiplicative inverses: Assume that $r \in R$ has a multiplicative inverse r^{-1} , and that $r' \in R$ is such that $r \cdot r' = 1$. Then multiply that latter equation by r^{-1} on the left to obtain

$$r^{-1} \cdot (r \cdot r') = r^{-1} \cdot 1 = r^{-1}$$

by the property of 1. Using the associativity of multiplication, the left-hand side is

$$r^{-1} \cdot (r \cdot r') = (r^{-1} \cdot r) \cdot r' = 1 \cdot r' = r'$$

by property of multiplicative inverses and of the identity. Putting this together, we have $r' = r^{-1}$ as desired.

The proof that $-(-r) = r$, that is, that the additive inverse of the additive inverse of r is just r , is identical to the argument given for *groups* that the inverse of the inverse is the original thing.

There are several ‘slogans’ that we all learned in high school or earlier, such as ‘minus times minus is plus’, and ‘zero times anything is zero’. It may be interesting to see that from the axioms for a ring we can *prove* those things. (We worried over the so-called ‘Laws of Exponents’ already a little earlier).

These things are a little subtler than the ‘obvious’ things above, insofar as they involve the interaction of the multiplication and addition.

And these little proofs are good models for how to prove simple general results about rings.

Let R be a ring.

- For any $r \in R$, $0 \cdot r = r \cdot 0 = 0$.
- Suppose that there is a 1 in R . Let -1 be the additive inverse of 1. Then for any $r \in R$ we have $(-1) \cdot r = r \cdot (-1) = -r$, where as usual $-r$ denotes the additive inverse of r .
- Let $-x, -y$ be the additive inverses of $x, y \in R$. Then $(-x) \cdot (-y) = xy$.

Proofs: Throughout this discussion, keep in mind that to prove that $b = -a$ means to prove just that $a + b = 0$.

Let’s prove that ‘zero times anything is zero’: Let $r \in R$. Then

$$\begin{aligned} 0 \cdot r &= (0 + 0) \cdot r && \text{(since } 0 + 0 = 0\text{)} \\ &= 0 \cdot r + 0 \cdot r && \text{(distributivity)} \end{aligned}$$

Then, adding $-(0 \cdot r)$ to both sides, we have

$$0 = 0 \cdot r - 0 \cdot r = 0 \cdot r + 0 \cdot r - 0 \cdot r = 0 \cdot r + 0 = 0 \cdot r$$

That is, $0 \cdot r$. The proof that $r \cdot 0 = 0$ is nearly identical.

Let’s show that $(-1) \cdot r = -r$. That is, we are asserting that $(-1)r$ is the additive inverse of r , which by now we know is unique. So all we have to do is check that

$$r + (-1)r = 0$$

We have

$$r + (-1)r = 1 \cdot r + (-1) \cdot r = (1 - 1) \cdot r = 0 \cdot r = 0$$

by using the property of 1, using distributivity, and using the result we just proved, that $0 \cdot r = 0$. We’re done.

Last, to show that $(-x)(-y) = xy$, we prove that $(-x)(-y) = -(-(xy))$, since we know generally that $-(-r) = r$. We can get halfway to the desired conclusion right now: we claim that $-(xy) = (-x)y$: this follows from the computation

$$(-x)y + xy = (-x + x)y = 0 \cdot y = 0$$

Combining these two things, what we want to show is that

$$(-x)(-y) + (-x)y = 0$$

Well,

$$(-x)(-y) + (-x)y = (-x)(-y + y) = (-x) \cdot 0 = 0$$

using distributivity and the property $r \cdot 0 = 0$. This proves that $(-x)(-y) = xy$.

18.2 Divisibility in rings

Before trying to prove that various commutative rings ‘have unique factorization’, we should make clear what this should mean. To make *this* clear, we need to talk about *divisibility* again. In this section we presume that any ring in question is *commutative* and has a *unit*.

The very first thing to understand is the potential failure of the possibility of the *cancellation property*, and its connection with the presence of non-zero zero divisors:

Theorem: A commutative ring R has the *cancellation property* if and only if it is an *integral domain*

Proof: Suppose that R has the cancellation property, and suppose that $r \cdot s = 0$. Since $r \cdot 0 = 0$ for any $r \in R$, we can write $r \cdot s = r \cdot 0$. For $r \neq 0$ we can cancel the r and obtain $s = 0$. Similarly, if $s \neq 0$ then $r = 0$. This shows that the cancellation property implies that there are no non-zero zero divisors.

On the other hand, suppose that R has no non-zero zero divisors. Suppose that $rz = rb$ with $r \neq 0$. Then, subtracting, $r(a - b) = 0$. Since $r \neq 0$, it must be that $a - b = 0$, or $a = b$. This is the desired cancellation property. ♣

In a commutative ring R , say that $x \in R$ **divides** $y \in R$ if there is $z \in R$ so that $y = zx$. And also say then that y is a **multiple** of x . And just as for the ordinary integers we may write

$$x|y$$

to say that x divides y . And then x is a **divisor** of y . If $xz = y$ and neither x nor z is a unit, then say that x is a **proper divisor** of y .

Keep in mind that since $r \cdot 0 = 0$ *anything* divides 0. But for the same reason 0 only divides *itself* and nothing else. On the other hand, if $u \in R$ is a *unit* in R (meaning that it has a multiplicative inverse in R) then u divides *everything*: let $r \in R$ be anything, and then we see that

$$r = r \cdot 1 = r \cdot (u^{-1} \cdot u) = (r \cdot u^{-1}) \cdot u$$

making clear that r is a multiple of u .

An element p in R is **prime** or **irreducible** if p itself is *not* a unit in R , but if $xy = p$ (with both $x, y \in R$) then either x or y is a *unit* in R .

A paraphrase of this is: an element is prime if and only if it has *no proper divisors*.

- If d is a *proper* divisor of a non-zero element r in an integral domain R , then

$$R \cdot r \subset R \cdot d$$

but

$$R \cdot r \neq R \cdot d$$

Proof: Since d is a divisor of r , there is $x \in R$ so that $xd = r$. Then

$$R \cdot r = R(xd) = (Rx)d \subset R \cdot d$$

since R is closed under multiplication, after all. Suppose that $R \cdot r = R \cdot d$. Then

$$d = 1 \cdot d \in R \cdot d = R \cdot r$$

so there is $s \in R$ so that $d = s \cdot r$. But then

$$r = xd = x(sr) = (xs)r$$

which gives $r(1 - xs) = 0$. Since $r \neq 0$ and R is an integral domain, $1 - xs = 0$ or $xs = 1$. That is, x is a unit, contradicting the assumption that $xd = r$ is a *proper* factorization of r . *Done*.

Two prime elements $p, q \in R$ are **associate** if there is a unit u in R so that $q = up$. (Since the inverse of a unit is of course a unit as well, this condition is symmetrical, being equivalent to the existence of a unit v so that $p = vq$).

The idea is that, for purposes of *factorization into primes*, two *associate* prime elements will be viewed as being essentially the same thing.

18.3 Polynomial rings

Another important and general construction of rings is **polynomial rings**: let R be a *commutative ring with unit*, and define

$$R[x] = \{ \text{polynomials with coefficients in } R \}$$

Then we use the usual addition and multiplication of polynomials. We will be especially interested in polynomials whose coefficients lie in a *field* k . By default, we might imagine that k is \mathbf{Q} or \mathbf{R} or \mathbf{C} , although we should also admit the possibility that the field k is a finite field such as \mathbf{Z}/p for p prime.

Let R be a commutative ring with unit 1. Let x be the thing we usually think of as a ‘variable’ or ‘indeterminate’. The **ring of polynomials in x with coefficients in R** is what it sounds like: the collection of all polynomials using indeterminate x and whose coefficients are in the ring R . This is also called the ring of polynomials in x **over** R . The notation for this is very standard: using *square brackets*:

$$R[x]$$

denotes the ring of polynomials over k . With the usual addition and multiplication of polynomials, this $R[x]$ is a *ring*.

We are most accustomed to polynomials with real numbers or complex numbers as coefficients, but there is nothing special about this.

When a polynomial with **indeterminate** x is written out as

$$P(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_3 x^3 + c_2 x^2 + c_1 x + c_0$$

the **coefficients** are the ‘numbers’ c_n, \dots, c_0 in the ring R . The **constant coefficient** is c_0 . If $c_n \neq 0$, then $c_n x^n$ is called the **highest-order-term** or **leading term** and c_n is the **highest-order coefficient** or **leading coefficient**.

We refer to the summand $c_i x^i$ as the **degree i term**. Also sometimes i is called the **order** of the summand $c_i x^i$. The order of the highest non-zero coefficient is the **degree** of the polynomial.

Remark: Sometimes people write a polynomial in the form above but *forget* to say whether c_n is definitely non-zero or not. Sometimes, also, people *presume* that if a polynomial is written in this fashion then c_n is non-zero, but that’s not safe at all.

A polynomial is said to be **monic** if its *leading* or *highest-order* coefficient is 1.

Remark: Sometimes polynomials are thought of as simply being a kind of *function*, but that is too naive generally. Polynomials *give rise to* functions, but they are more than just that. It is true that a polynomial

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0$$

with coefficients in a ring R gives rise to functions on the ring R , writing as usual

$$f(a) = c_n a^n + c_{n-1} a^{n-1} + \dots + c_1 a + c_0$$

for $a \in R$. That is, as usual, we imagine that the ‘indeterminate’ x is replaced by a everywhere (or “ a is substituted for x ”). This procedure gives functions from R to R .

But polynomials themselves have features which may become invisible if we mistakenly think of them as just being functions. For example, suppose that we look at the polynomial $f(x) = x^3 + x^2 + x + \bar{1}$ in the polynomial ring $(\mathbf{Z}/2)[x]$, that is, with coefficients in $\mathbf{Z}/2$. Then

$$f(\bar{0}) = \bar{0}^3 + \bar{0}^2 + \bar{0} + \bar{1} = \bar{0}$$

$$f(\bar{1}) = \bar{1}^3 + \bar{1}^2 + \bar{1} + \bar{1} = \bar{0}$$

That is, the *function* attached to the polynomial is the 0-function, but the polynomial is visibly not the zero polynomial.

As another example, consider $f(x) = x^3 - x$ as a polynomial with coefficients in $\mathbf{Z}/3$. Once again, $f(\bar{0})$, $f(\bar{1})$, $f(\bar{2})$, are all $\bar{0}$, but the polynomial is certainly not the zero polynomial.

18.4 Euclidean algorithm for polynomials

In a polynomial ring $k[x]$ with k a *field*, there is a **Division Algorithm** and (therefore) there is a **Euclidean Algorithm** nearly identical *in form* to the analogous algorithms in the ordinary integers \mathbf{Z} .

The division algorithm is just the usual *division of one polynomial by another*, with remainder, as we all learned in high school or earlier. It takes just a moment’s reflection to see that the procedure we all learned does *not* depend upon the nature of the field that the coefficients are in, and that the degree of the remainder is indeed less than the degree of the divisor!

For example: let’s reduce $x^3 + 1$ modulo $x^2 + 1$:

$$(x^3 + 1) - x \cdot (x^2 + 1) = x - 1$$

We’re done with the reduction because the degree of $x - 1$ is (strictly) less than the degree of $x^2 + 1$. Reduce $x^5 + 1$ modulo $x^2 + 1$, in stages:

$$(x^5 + 1) - x^3 \cdot (x^2 + 1) = -x^3 + 1$$

$$(-x^3 + 1) + x \cdot (x^2 + 1) = x + 1$$

which, summarized, gives the reduction

$$(x^5 + 1) - (x^3 - x) \cdot (x^2 + 1) = x + 1$$

Next, since the division algorithm works for polynomials with coefficients in a field, it is merely a *corollary* that we have a ‘Euclidean algorithm’! If we think about it, the crucial thing in having the Euclidean

algorithm work was that the division algorithm gave us progressively smaller numbers at each step. (And, indeed, each step of the Euclidean Algorithm is just the Division Algorithm!)

18.5 Euclidean rings

Based on our the most important examples of rings with a *Division Algorithm* and therefore with a *Euclidean Algorithm*, the ordinary integers and polynomials over a field, we now abstract the crucial property which makes this work. The goal is only to prove that *Euclidean rings have the Unique Factorization property*.

This whole line of argument applies to the ordinary integers as well, so we finally will have *proven* what we perhaps had been taking for granted all along, namely that the ordinary integers really do have unique factorizations into primes.

An **absolute value** on a commutative ring R is a function usually denoted $|r|$ of elements $r \in R$ having the properties

- *Multiplicativity*: For all $r, s \in R$ we have $|rs| = |r| \cdot |s|$.
- *Triangle inequality*: For all $r, s \in R$ we have $|r + s| \leq |r| + |s|$.
- *Positivity*: If $|r| = 0$ then $r = 0$.

If an absolute value on a ring R has the property that *any non-empty subset S of R has an element of least positive absolute value* (among the collection of absolute values of elements of S), then we say the the absolute value is **discrete**.

A commutative ring R with unit is **Euclidean** if there is a *discrete* absolute value on it, denoted $|r|$, so that for any $x \in R$ and for any $0 \neq y \in R$ there are $q, r \in R$ so that

$$x = yq + r \quad \text{with } |r| < |y|$$

The idea is that *we can divide and get a remainder strictly smaller than the divisor*.

The hypothesis that the absolute value be *discrete* in the above sense is critical. Sometimes it is easy to see that this requirement is fulfilled. For example, if $|\cdot|$ is *integer-valued*, as is the case with the usual absolute value on the ordinary integers, then the usual Well-Ordering Principle assures the ‘discreteness’.

The most important examples of Euclidean rings are the ordinary integers \mathbf{Z} and any polynomial ring $k[x]$ where k is a field. The absolute value in \mathbf{Z} is just the usual one, while we have to be a tiny bit creative in the case of polynomials, and define

$$|P(x)| = 2^{\text{degree } P}$$

And $|0| = 0$. Here the number 2 could be replaced by any other number bigger than 1, and the absolute value obtained would work just as well.

- A Euclidean ring R is an *integral domain*.

Proof: We must show that R has no *zero-divisors*, that is, we must show that if $xy = 0$ then either x or y is 0. Well, if $xy = 0$ then

$$0 = |0| = |xy| = |x| \cdot |y|$$

by the multiplicative property of the norm. Now $|x|$ and $|y|$ are non-negative real numbers, so for their product to be 0 one or the other of $|x|$ and $|y|$ must be 0. And then by the positivity property of the norm it must be that one of x, y themselves is 0, as claimed. ♣

- In a Euclidean ring R , if $r \in R$ has $|r| < 1$ then $r = 0$.

Proof: Since $|ab| = |a| \cdot |b|$, we have $|r^n| = |r|^n$. If $r \neq 0$, the powers $|r|^n$ form a set of values of the absolute value which have no *least* value: they form a decreasing sequence with limit 0, but the sequence does not *contain* 0. Thus, $r = 0$. ♣

- In a Euclidean ring R , an element $u \in R$ is a *unit* (that is, has a multiplicative inverse) if and only if $|u| = 1$. In particular, $-1 = 1$.

Proof: First, since $1 \cdot 1 = 1$, by taking absolute values and using the multiplicative property of the absolute value, we have

$$|1| = |1 \cdot 1| = |1| \cdot |1|$$

The only real numbers z with the property that $z = z^2$ are 0 and 1, and since $1 \neq 0$ we have $|1| \neq 0$, so necessarily $|1| = 1$. If $uv = 1$, then, by taking absolute values, we have $1 = |uv| = |u| \cdot |v|$. Since the only ring element with absolute value strictly smaller than 1 is 0 (from just above), we conclude that both $|u|$ and $|v|$ are ≥ 1 . Therefore, since their product is 1, they must both be 1. So the absolute value of a unit is 1. On the other hand, suppose $|u| = 1$. Then, applying the division/reduction algorithm, we reduce 1 itself to get

$$1 = q \cdot u + r$$

with $|r| < |u|$. Since $|u| = 1$, $|r| < 1$. But from above we know that this implies $r = 0$. So $1 = qu$, and q is the multiplicative inverse to u . So anything with absolute value 1 is a unit. ♣

Theorem: For x, y in a Euclidean ring R , an element of the form $sx + ty$ (for $s, t \in R$) with smallest absolute value is a *gcd* of x, y .

Proof: The discreteness hypothesis on the absolute value assures that among the *non-zero* values $|sx + ty|$ there is at least one which is minimal. Let $sx + ty$ be such. We must show that $g|x$ and $g|y$. Using the division/reduction algorithm, we have

$$x = q(sx + ty) + r$$

with $|r| < |sx + ty|$. Rearranging the equation, we obtain

$$r = (1 - qs)x + (-qt)y$$

So r itself is of the form $s'x + t'y$ with $s', t' \in R$. Since $sx + ty$ had the smallest non-zero absolute value of any such thing, and $|r| < |sx + ty|$, it must be that $r = 0$. So $sx + ty$ divides x . Similarly, $sx + ty$ must divide y . This proves that $sx + ty$ is a divisor of both x and y . On the other hand, $d|x$ and $d|y$, then certainly $d|sx + ty$. ♣

Proposition: In a Euclidean ring R , an element $p \in R$ is prime if $d|p$ implies $|d| = 1$ or $|d| = |p|$. That is, a *proper* divisor d of $r \in R$ has the property that $1 < |d| < |r|$.

Proof: Recall that the definition of a prime element p in a commutative ring R is that if $ab = p$ then either a or b is a unit. To prove both statements of the proposition, it suffices to prove that if $ab = n$ with *neither* a nor b a unit, then $1 < |a| < |n|$. On one hand, if $1 < |a| < |n|$ then, because $|n| = |ab| = |a| \cdot |b|$, $|n| > |b| > 1$. Thus, since the units of R are exactly those elements with absolute value 1, neither a nor b is a unit. On the other hand, if $ab = n$ and neither a nor b is a unit, then $1 < |a|$ and $1 < |b|$. Since $|n| = |ab| = |a| \cdot |b|$, it follows that also $|a| < |n|$ and $|b| < |n|$. ♣

Key Lemma: Let p be a prime element in a Euclidean ring R . If $p|ab$ then $p|a$ or $p|b$. Generally, if a prime p divides a product $a_1 \dots a_n$ then p must divide one of the factors a_i .

Proof: It suffices to prove that if $p|ab$ and $p \nmid a$ then $p|b$. Since $p \nmid a$, and since p is prime, the *gcd* of p and a is just 1. Therefore, there are $s, t \in R$ so that

$$1 = sa + tp$$

Then

$$b = b \cdot 1 = b \cdot (sa + tp) = s(ab) + (bt)p$$

Since $p|ab$, surely p divides the right-hand side. Therefore, $p|b$, as claimed.

Generally, if p divides $a_1 \dots a_n$, rewrite this as $(a_1)(a_2 \dots a_n)$. By the first part, either $p|a_1$ or $p|a_2 \dots a_n$. In the former case we're done. In the latter case, we continue: rewrite $a_2 \dots a_n = (a_2)(a_3 \dots a_n)$. So either $p|a_2$ or $p|a_3 \dots a_n$. Continuing (induction!), we find that p divides at least one of the factors a_i . ♣

Theorem: In a Euclidean ring R , every element $r \in R$ can be factored into primes as

$$r = up_1^{e_1} \dots p_m^{e_m}$$

where u is a unit, the p_i are distinct primes, and the e_i are positive integers. If

$$r = vq_1^{f_1} \dots q_n^{f_n}$$

is another such factorization, with unit v and primes q_i , then $m = n$, and we can reorder and relabel the q_i 's so that

$$q_i = p_i \times u_i$$

for some unit u_i , for all indices i . And $e_i = f_i$. That is, the factorization into primes is **essentially unique**.

Proof: First we prove the *existence* of factorizations into primes. Suppose that some $r \in R$ did not have a factorization. Then, invoking the discreteness, there is a $r \in R$ without a factorization and with $|r|$ *smallest* among all elements lacking a prime factorization. If r is prime, then of course it has a factorization, so such r can't be prime. But then r has a proper factorization $r = ab$. Just above, we saw that this means that $1 < |a| < |r|$ and $1 < |b| < |r|$. Since $|a| < |r|$ and $|b| < |r|$, by the minimality of r it must be that both a and b have prime factorizations. Then a prime factorization of r would be obtained by multiplying together the prime factorizations for a and b . (The product of two units is again a unit!).

Now we prove uniqueness of the factorization. Suppose that

$$r = u \cdot p_1^{e_1} \dots p_m^{e_m}$$

and also

$$r = v \cdot q_1^{f_1} \dots q_n^{f_n}$$

with primes p_i and q_i . By induction, we could assume that m is the *smallest* integer for which there is a *different* factorization. Since p_1 divides $vq_1^{f_1} \dots q_n^{f_n}$ and p_1 is prime, by the Key Lemma above p_1 must divide one of the q_i . By relabelling the q_i 's, we may suppose that $p_1|q_1$. Since these are both prime, they must differ by a unit, that is, there is a unit u_1 so that $q_1 = u_1 \cdot p_1$. Replacing q_1 by $u_1 p_1$, we get

$$up_1^{e_1} \dots p_m^{e_m} = vu_1^{f_1} \cdot p_1^{f_1} q_2^{f_2} q_3^{f_3} \dots q_n^{f_n}$$

Note that $vu_1^{f_1}$ is still a unit. Since $e_1 \geq 1$ and $f_1 \geq 1$, we can *cancel* at least one factor of p_1 from both sides. (We have already proven that a Euclidean ring is an integral domain).

But by induction, since we assumed that m was the smallest integer occurring in an expression of some $r \in R$ in two different ways, after removing the common factor of p_1 the remaining factorizations must be essentially the same. (That is, after adjusting the primes by units if necessary, they and their exponents all match). ♣

A person might notice that we didn't use the triangle inequality at all in these proofs. That is indeed so, but in practice anything which is a reasonable candidate for an 'absolute value' in the axiomatic sense suggests itself mostly because it *does* behave like an absolute value in a more down-to-earth sense, which includes a triangle inequality.

#18.145 Let $k[x]$ be the polynomial ring in one variable x over the field k . What is the group of units $k[x]^\times$?

#18.146 Find the greatest common divisor of $x^5 + x^4 + x^3 + x^2 + x + 1$ and $x^4 + x^2 + 1$, viewed as elements in the ring $\mathbf{Q}[x]$ of polynomials over \mathbf{Q} .

#18.147 Find the greatest common divisor of $x^6 + x^3 + 1$ and $x^2 + x + 1$, viewed as elements in the ring $k[x]$ of polynomials over the finite field $k = \mathbf{Z}/3$ with 3 elements.

#18.148 Find the greatest common divisor of $x^6 + x^4 + x^2 + 1$ and $x^8 + x^6 + x^4 + x^2 + 1$, viewed as elements in the ring $k[x]$ of polynomials over the finite field $k = \mathbf{Z}/2$ with 2 elements.

#18.149 Find the greatest common divisor of $x^4 + 5x^3 + 6x^2 + 5x + 1$ and $x^4 + 1$, viewed as having coefficients in $\mathbf{Z}/7$.

#18.150 Find the greatest common divisor of $x^4 + 2x^2 + x + 2$ and $x^4 + 1$, viewed as having coefficients in $\mathbf{Z}/3$.

#18.151 Even though $x^6 + 3x^5 + 3x^4 + x^3 + 3x^2 + 3x + 4$ has no roots in $\mathbf{Z}/5$, it has a repeated factor. Find it.

#18.152 Even though $x^6 + 4x^5 + 6x^4 + 3x^3 + 2x + 4$ has no roots in $\mathbf{Z}/7$, it has a repeated factor. Find it.

#18.153 Let u be a unit in a commutative ring R . Show that no non-unit in R can *divide* u .

#18.154 Show that in a ring if $x = yu$ with a unit u then $y = xu'$ for some unit u' .

19. Cyclotomic polynomials

- Characteristics of fields
 - Multiple factors in polynomials
 - Cyclotomic polynomials
 - Primitive roots in finite fields
-

19.1 Characteristics of fields

Let k be a field. The **characteristic** $\text{char } k$ of k is the smallest positive integer n (if there *is* one) so that

$$\underbrace{1_k + 1_k + \dots + 1_k}_n = 0_k$$

where 1_k is the unit in k and 0_k is the zero. As usual, we abbreviate

$$\ell \cdot 1_k = \underbrace{1_k + 1_k + \dots + 1_k}_\ell$$

for positive integers ℓ .

If there is *no* such positive integer n , then the characteristic is said to be 0. Thus,

$$\text{char } \mathbf{Q} = 0$$

By contrast,

$$\text{char } \mathbf{Z}/p = p$$

Proposition: The characteristic of a field is a prime number, if it is non-zero. For a field of characteristic p with p prime, if for some positive integer n

$$\underbrace{1_k + 1_k + \dots + 1_k}_n = 0_k$$

then p divides n .

Proof: Suppose that

$$\underbrace{1_k + 1_k + \dots + 1_k}_n = 0_k$$

with n *minimal* to achieve this effect, and that n had a factorization

$$n = a \cdot b$$

with positive integers a and b . Then

$$\underbrace{(1_k + 1_k + \dots + 1_k)}_a \cdot \underbrace{(1_k + 1_k + \dots + 1_k)}_b = \underbrace{1_k + 1_k + \dots + 1_k}_n = 0_k$$

Since a field has no proper zero-divisors, it must be that either $a \cdot 1_k = 0$ or $b \cdot 1_k = 0$. By the hypothesis that n was minimal, if $a \cdot 1_k = 0$ then $a = n$, and similarly for b . Thus, the factorization $n = a \cdot b$ was not *proper*. Since n has no proper factorization, it is prime.

Suppose that $n \cdot 1_k = 0_k$. By the division algorithm, we have $n = qp + r$ with $0 \leq r < p$. Then

$$0_k = n \cdot 1_k = q(p \cdot 1_k) + r \cdot 1_k = 0_k + r \cdot 1_k$$

From this, $r \cdot 1_k = 0_k$. Since $r < p$ and p was the least positive integer with $p \cdot 1_k = 0_k$, it follows that $r = 0$ and p divides n . ♣

Fields with positive characteristic p have a peculiarity which is at first counter-intuitive, but which plays an important role in both theory and applications:

Proposition: Let k be a field of positive characteristic p . Then for any polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$$

in $k[x]$ we have

$$f(x)^p = a_n^p x^{pn} + a_{n-1}^p x^{p(n-1)} + \dots + a_2^p x^{2p} + a_1^p x^p + a_0^p$$

Proof: Recall that p divides binomial coefficients $\binom{p}{i}$ with $0 < i < p$. Therefore, for $0 < i < p$,

$$\binom{p}{i} \cdot 1_k = 0 + k$$

Thus, for $a_n \in k$ and any polynomial $g(x)$ with coefficients in k ,

$$(a_n x^n + g(x))^p = (a_n x^n)^p + \sum_{0 < i < p} \binom{p}{i} (a_n x^n)^{p-i} g(x)^i + g(x)^p$$

All the middle terms have a coefficient

$$\binom{p}{i} \cdot 1_k = 0_k$$

so they disappear. Thus,

$$(a_n x^n + g(x))^p = a_n^p x^{pn} + g(x)^p$$

The same assertion applies to $g(x)$ itself. Take

$$g(x) = a_{n-1} x^{n-1} + h(x)$$

Then

$$g(x)^p = a_{n-1}^p x^{p(n-1)} + h(x)^p$$

Continuing (that is, doing an induction), we obtain the result for f . ♣

For example, with coefficients in $k = \mathbf{Z}/p$ with p prime, we have

$$(x + 1)^p = x^p + \sum_{0 < i < p} \binom{p}{i} x^i + 1 = x^p + 1$$

Also

$$(x^2 + 1)^p = x^{2p} + 1$$
$$(x^2 + x + 1)^p = x^{2p} + x^p + 1$$

and such things.

19.2 Multiple factors in polynomials

There is a very simple device to detect repeated occurrence of a factor in polynomial (with coefficients in a field). This is very useful both theoretically and in computational situations.

Let k be a *field*. For a polynomial

$$f(x) = c_n x^n + \dots c_1 x + c_0$$

with coefficients c_i in k , we *define*

$$f'(x) = n c_n x^{n-1} + (n-1)c_{n-1}x^{n-2} + \dots + 3c_3x^2 + 2c_2x + c_1$$

Remark: Note that we simply *define* a “derivative” this way, purely algebraically, without taking any limits. Of course (!) this formula is still supposed to yield a thing with familiar properties, such as the product rule. So we’ve simply used our calculus experience to make a “good guess”.

Lemma: For two polynomials f, g in the ring $k[x]$ of polynomials in x with coefficients in k , and for $r \in k$,

- $(r \cdot f)' = r \cdot f'$
- $(f + g)' = f' + g'$
- $(fg)' = f'g + fg'$

Proof: The first assertion is easy: let $f(x) = a_m x^m + \dots + a_0$, and compute

$$\begin{aligned} (r \cdot (a_m x^m + \dots + a_0))' &= (r a_m x^m + r a_{m-1} x^{m-1} + \dots + r a_0)' \\ &= m \cdot (r a_m) x^{m-1} + (m-1) \cdot (r a_{m-1}) x^{m-2} + \dots + r a_1 + 0 \\ &= r(m \cdot (a_m) x^{m-1} + (m-1) \cdot (a_{m-1}) x^{m-2} + \dots + a_1 + 0) = r \cdot f'(x) \end{aligned}$$

The second assertion is also not hard: let $f(x) = a_m x^m + \dots + a_0$ and $g(x) = b_n x^n + \dots + b_0$. Padding the one of smaller degree with terms of the form $0 \cdot x^\ell$, we can suppose without loss of generality that $m = n$. (This simplifies notation considerably!) Then

$$\begin{aligned} (f(x) + g(x))' &= ((a_n + b_n)x^n + \dots + \dots + (a_1 + b_1)x + (a_0 + b_0)x^0)' \\ &= n(a_n + b_n)x^{n-1} + (n-1)(a_{n-1} + b_{n-1})x^{n-2} + \dots + 1(a_1 + b_1)x^0 + 0 \cdot x^0 \\ &= (n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots + 1 \cdot a_1 x^0) + (n b_n x^{n-1} + \dots + (n-1)b_{n-1}x^{n-2} + \dots + 1 \cdot b_1 x^0) \\ &= f'(x) + g'(x) \end{aligned}$$

For the third, property, let's first see what happens when f and g are *monomials*, that is, are simply $f(x) = ax^m$, $g(x) = bx^n$. On one hand, we have

$$(fg)' = (ax^m \cdot bx^n)' = (abx^{m+n})' = ab(m+n)x^{m+n-1}$$

On the other hand,

$$f'g + fg' = amx^{m-1} \cdot bx^n + ax^m \cdot bnx^{n-1} = ab(m+n)x^{m+n-1}$$

after simplifying. This proves the product rule for monomials.

To approach the general product rule, let

$$f(x) = a_mx^m + \dots + a_o$$

$$g(x) = b_nx^n + \dots + b_o$$

The coefficient of x^ℓ in the product $f(x)g(x)$ is

$$\sum_{i+j=\ell} a_i \cdot b_j$$

Then the coefficient of $x^{\ell-1}$ in the derivative of the product is

$$\ell \sum_{i+j=\ell} a_i \cdot b_j$$

On the other hand, the coefficient of $x^{\ell-1}$ in $f'g$ is

$$\sum_{i+j=\ell} (ia_i) \cdot b_j$$

and the coefficient of $x^{\ell-1}$ in fg' is

$$\sum_{i+j=\ell} a_i \cdot jb_j$$

Adding these two together, we find that the coefficient of $x^{\ell-1}$ in $f'g + fg'$ is

$$\sum_{i+j=\ell} a_i \cdot b_j \cdot (i+j) = \ell \sum_{i+j=\ell} a_i \cdot b_j$$

which matches the coefficient in $(fg)'$. This proves the product rule. ♣

Proposition: Let f be a polynomial with coefficients in a field k . Let P be an irreducible polynomial with coefficients in k . Then P^2 divides f if and only if P divides $\gcd(f, f')$.

Proof: On one hand, suppose $f = P^2 \cdot g$. Then, using the product rule,

$$f' = 2PP' \cdot g + P^2 \cdot g' = P \cdot (2P'g + Pg')$$

which is certainly a multiple of P . This half of the argument did not use the irreducibility of P .

On the other hand, suppose that P divides both f and f' (and show that actually P^2 divides f). Dividing f/P by P , we obtain

$$f/P = Q \cdot P + R$$

with the degree of R less than that of P . Then $f = QP^2 + RP$. Taking the derivative, we have

$$f' = Q'P^2 + 2QP P' + R'P + RP'$$

By hypothesis P divides f' . All the terms on the right-hand side except possibly RP' are divisible by P , so P divides RP' . Since P is irreducible and it divides the product RP' , it must divide either R or P' . If it divides R , then we've shown that P^2 divides f , so we're done.

If P fails to divide R then P must divide P' . Since P' is of lower degree than P , if P divides it then P' must be the zero polynomial. Let's see that this is impossible for P irreducible. Let

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$$

Then

$$P'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x^1 + a_1 + 0$$

For this to be the zero polynomial it must be that

$$\ell \cdot a_\ell = 0$$

for all indices ℓ . That is, for any index ℓ with $a_\ell \neq 0$ it must be that $\ell \cdot 1_k = 0_k$. Since at least one coefficient of P is non-zero, this implies that the *characteristic* of k is not 0, so from above is some prime p . From above, $\ell \cdot 1_k = 0_k$ implies that p divides ℓ . That is, the characteristic p divides ℓ if the coefficient a_ℓ is non-zero. So we can write

$$f(x) = a_{pm} x^{pm} + a_{p(m-1)} x^{p(m-1)} + a_{p(m-2)} x^{p(m-2)} + \dots + a_{2p} x^{2p} + a_p x^p + a_0$$

From above, we recognize this as the p^{th} power of

$$a_{pm} x^n + a_{p(m-1)} x^{(m-1)} + a_{p(m-2)} x^{(m-2)} + \dots + a_{2p} x^2 + a_p x + a_0$$

But if P is a p^{th} power it is certainly not irreducible. Therefore, for P irreducible it cannot be that P' is the zero polynomial. Therefore, above it must have been that $R = 0$, which is to say that P^2 divides f , as claimed. ♣

19.3 Cyclotomic polynomials

For b in a field k , the **exponent** of b is the smallest positive integer n (if it exists at all) so that $b^n = 1$. That is, $b^n = 1$ but $b^d \neq 1$ for $0 < d < n$. In other words, b is a root of the polynomial $x^n - 1$ but not of $x^d - 1$ for any smaller d . What we'll do here is describe the polynomial φ_n , the n^{th} **cyclotomic polynomial**, of which b must be a root in order to have exponent n .

Fix a field k , and an integer n *not* divisible by the characteristic of k . (If the characteristic is 0 then this is no condition at all.)

Lemma: For m, n two integers (divisible by the characteristic or not)

$$\gcd(x^m - 1, x^n - 1) = x^{gcd(m,n)} - 1$$

$$\text{lcm}(x^m - 1, x^n - 1) = x^{lcm(m,n)} - 1$$

Proof: We do induction on the maximum of m and n . First, if by chance $m = n$, then $x^m - 1 = x^n - 1$ and we are certainly done. Second, if $m > n$, doing a fragment of a division, we have

$$x^m - 1 - x^{m-n} \cdot (x^n - 1) = x^{m-n} - 1$$

So if D is a polynomial dividing both $x^m - 1$ and $x^n - 1$ then D divides $x^{m-n} - 1$ as well. By induction,

$$\gcd(x^{m-n} - 1, x^n - 1) = x^{\gcd(m-n, n)} - 1$$

But

$$\gcd(m, n) = \gcd(m - n, n)$$

and

$$x^m - 1 = x^{m-n} \cdot (x^n - 1) + x^{m-n} - 1$$

so

$$\gcd(x^m - 1, x^n - 1) = \gcd(x^{m-n} - 1, x^n - 1)$$

If $m < n$ we reverse the roles of m and n : let's repeat the argument. Doing a fragment of a division:

$$x^n - 1 - x^{n-m} \cdot (x^m - 1) = x^{n-m} - 1$$

So if D is a polynomial dividing both $x^m - 1$ and $x^n - 1$ then D divides $x^{n-m} - 1$ as well. By induction,

$$\gcd(x^{n-m} - 1, x^n - 1) = x^{\gcd(n-m, n)} - 1$$

But

$$\gcd(m, n) = \gcd(n - m, n)$$

and

$$x^n - 1 = x^{n-m} \cdot (x^m - 1) + x^{n-m} - 1$$

so

$$\gcd(x^m - 1, x^n - 1) = \gcd(x^{n-m} - 1, x^m - 1)$$

This completes the induction step. (The discussion of the least common multiple is essentially identical, and also follows from this discussion.) 

Lemma: Let n be a positive integer not divisible by the characteristic of the field k . Then the polynomial $x^n - 1$ has no repeated factors.

Proof: From above, it suffices to check that the \gcd of $x^n - 1$ and its derivative nx^{n-1} is 1. Since the characteristic of the field does not divide n , $n \cdot 1_k$ has a multiplicative inverse t in k . Then, doing a division with remainder,

$$(x^n - 1) - t(nx^{n-1}) = -1$$

Thus, the \gcd is 1. 

Now suppose that n is not divisible by the characteristic of the field k , and define the n^{th} **cyclotomic polynomial** $\varphi_n(x)$ (with coefficients in k) by

$$\varphi_n(x) = \frac{x^n - 1}{\text{lcm of all } x^d - 1 \text{ with } 0 < d < n, d \text{ dividing } n}$$

where the least common multiple is taken to be *monic*.

Theorem: Let $m = n$ be integers neither of which is divisible by the characteristic of the field k . Then

- φ_n is monic
- $\gcd(\varphi_m, \varphi_n) = 1$.
- The degree of φ_n is $\varphi(n)$ (Euler's phi-function)
- There is a more efficient description of $\varphi_n(x)$:

$$ph_n(x) = \frac{x^n - 1}{\prod_{1 \leq d < n, d|n} \varphi_d(x)}$$

- The polynomial $x^n - 1$ factors as

$$x^n - 1 = \prod_{1 \leq d \leq n, d|n} \varphi_d(x)$$

Proof: First, we really should check that the least common multiple of the $x^d - 1$ with $d < n$ and $d|n$ divides $x^n - 1$. We know that $d|n$ (and $d > 0$) implies that $x^d - 1$ divides $x^n - 1$ (either by high school algebra or from the lemma above). Therefore, using *unique factorization* of polynomials with coefficients in a field, it follows that the least common multiple of a collection of things each dividing $x^n - 1$ will also divide $x^n - 1$.

Next, the assertion that φ_n is *monic* follows from its definition, since it is the quotient of the monic polynomial $x^n - 1$ by the monic *lcm* of polynomials.

Next, to determine the *gcd* of φ_m and φ_n , first observe that φ_m divides $x^m - 1$ and φ_n divides $x^n - 1$, so

$$\gcd(\varphi_m, \varphi_n) \text{ divides } \gcd(x^m - 1, x^n - 1)$$

In the lemma above we computed that

$$\gcd(x^m - 1, x^n - 1) = x^{gcd(m,n)} - 1$$

But from its definition, φ_m divides

$$\frac{x^m - 1}{x^{gcd(m,n)} - 1}$$

so $\gcd(\varphi_m, \varphi_n)$ also divides this. Since n is not divisible by the characteristic, the lemma above shows that $x^n - 1$ has no repeated factors. Therefore, from the fact that $\gcd(\varphi_n, \varphi_m)$ divides $x^{gcd(m,n)} - 1$ and also divides $(x^n - 1)/(x^{gcd(m,n)} - 1)$ we conclude that $\gcd(x^m - 1, x^n - 1) = 1$.

Next, we use induction to prove that

$$x^n - 1 = \prod_{1 \leq d \leq n, d|n} \varphi_d(x)$$

For $n = 1$ the assertion is true. From the definition of φ_n , we have

$$x^n - 1 = \varphi_n(x) \cdot \text{lcm}\{x^d - 1 : d|n, 0 < d < n\}$$

By induction, for $d < n$

$$x^d - 1 = \prod_{0 < e < d, e|d} \varphi_e(x)$$

Since we have already shown that for $m \neq n$ the *gcd* of φ_m and φ_n is 1, we have

$$\text{lcm}\{x^d - 1 : d|n, 0 < d < n\} = \prod_{d|n, d < n} \varphi_d(x)$$

Thus,

$$x^n - 1 = \varphi_n(x) \cdot \prod_{d|n, d < n} \varphi_d(x)$$

as claimed.

The assertion about the degree of φ_n follows from the identity proven earlier for Euler's phi-function:

$$\sum_{d|n, d > 0} \varphi(d) = n$$

This completes the proof of the theorem. ♣

19.4 Primitive roots in finite fields

Now we can prove that the multiplicative group k^\times of the any finite field k is a *cyclic group*. A generator of k^\times is sometimes called a *primitive root* for k . This property of k^\times is essential for the working of modern primality tests and modern factorization algorithms.

Theorem: Let k be a finite field. Then k^\times is a cyclic group.

Proof: Let q be the number of elements in k . The group of units k^\times is a group. Since k is a field, any $b \neq 0$ has a multiplicative inverse in k . So the order of k^\times is $q - 1$. Thus, by corollaries to Lagrange's theorem, for $b \neq 0$,

$$b^{q-1} = 1$$

That is, any non-zero element of k is a root of the polynomial $f(x) = x^{q-1} - 1$. On the other hand, by the Fundamental Theorem of Algebra, this polynomial has at most $q - 1$ roots in k . Therefore, it has *exactly* $q - 1$ (distinct) roots in k .

Let p be the characteristic of k . Certainly p cannot divide $q - 1$, since if it did then the derivative of $f(x) = x^{q-1} - 1$ would be zero, so $\gcd(f, f') = f$ and f would have multiple roots. We have just noted that f has $q - 1$ distinct roots, so this doesn't happen.

Since the characteristic of k does not divide $q - 1$, we can apply the results from just above concerning cyclotomic polynomials. Thus,

$$x^{q-1} - 1 = \prod_{d|q-1} \varphi_d(x)$$

Since $x^{q-1} - 1$ has $q - 1$ roots in k , and since the φ_d 's here are relatively prime to each other, each φ_d with $d|q - 1$ must have number of roots (in k) equal to its degree. Thus, φ_d for $d|q - 1$ has $\varphi(d) > 0$ roots in k (Euler's phi-function).

Finally, the roots of $\varphi_{q-1}(x)$ are those field elements b so that $b^{q-1} = 1$ and no smaller positive power than $q - 1$ has this property. The primitive roots are exactly the roots of $\varphi_{q-1}(x)$. The cyclotomic polynomial φ_{q-1} has $\varphi(q - 1)$ roots. Therefore, there are $\varphi(q - 1) > 0$ primitive roots. That is, the group k^\times has a generator, that is, is cyclic. ♣

#19.155 Determine the cyclotomic polynomials $\varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6, \varphi_8, \varphi_9, \varphi_{12}$.

#19.156 (*) Find a cyclotomic polynomial that has coefficients other than 0, +1, -1.

20. Primitive roots

- Primitive roots in \mathbf{Z}/p
 - Primitive roots in \mathbf{Z}/p^e
 - Counting primitive roots
 - Non-existence of primitive roots
-

20.1 Primitive roots in \mathbf{Z}/p

Now we can verify that the multiplicative group \mathbf{Z}/p^\times of the finite field \mathbf{Z}/p with p elements is a *cyclic group*. Any generator of it is called a *primitive root* for \mathbf{Z}/p . This property of \mathbf{Z}/p (and other finite fields) is essential in primality tests and factorization algorithms.

Theorem: Let k be the finite field \mathbf{Z}/p with p prime. Then \mathbf{Z}/p^\times is a cyclic group.

Proof: As corollary of our study of cyclotomic polynomials, we've already proven that the multiplicative group k^\times of any finite field k is cyclic. Therefore, all we need do is check that \mathbf{Z}/p is a field. That is, we must check that any non-zero element $b \in \mathbf{Z}/p$ has a multiplicative inverse.

Let's repeat the explanation of why there is a multiplicative inverse, even though we've given it before in other contexts. Indeed, since p is prime, if $b \neq 0 \pmod p$, then $\gcd(p, b) = 1$. Thus, there are integers s, t so that $sp + tb = 1$. Then, looking at the latter equation modulo p , we see that t is a multiplicative inverse to b modulo p . ♣

20.2 Primitive roots in \mathbf{Z}/p^e

To prove that there is a primitive root in \mathbf{Z}/p^e for p an odd prime is not difficult, once we know that there is a primitive root for \mathbf{Z}/p . A minor adaption of this applies as well to $\mathbf{Z}/2p^e$.

Theorem: For an odd prime p , \mathbf{Z}/p^e and $\mathbf{Z}/2p^e$ have primitive roots. That is, the multiplicative groups \mathbf{Z}/p^{e^\times} and $\mathbf{Z}/2p^{e^\times}$ are *cyclic*.

Corollary: (*of proof*) In fact, for an integer g which is a primitive root mod p , either g is a primitive root mod p^e and mod $2p^e$ for all $e \geq 1$, or else $(1+p)g$ is. In particular, if $g^{p-1} \neq 1 \pmod{p^2}$, then g is a primitive root mod p^e and mod $2p^e$ for all $e \geq 1$. Otherwise, $(1+p)g$ is.

The following proposition is of interest in its own right, and is necessary to prove the theorem on primitive roots. Its point is that understanding the order of *certain* types of elements in \mathbf{Z}/p^{e^\times} is much more elementary than the trouble we went through to show that \mathbf{Z}/p has a primitive root. We'll prove this proposition before proving the theorem and corollary on primitive roots.

Proposition: Let p be an odd prime. For integers $1 \leq k \leq e$, and for an integer x with $p \nmid x$, the order of an element $1 + p^k x$ in $\mathbf{Z}/p^{e \times}$ is p^{e-k} . In particular, for $p \nmid x$ and $k \geq 1$,

$$(1 + p^k x)^{p^\ell} = 1 + p^{k+\ell} y$$

with $y = x \pmod p$.

Proof: (of proposition). The main trick here is that a prime p divides the binomial coefficients

$$\binom{p}{1}, \binom{p}{2}, \dots, \binom{p}{p-2}, \binom{p}{p-1}$$

Also, the hypothesis that $p > 2$ is essential.

Let's first compute

$$\begin{aligned} (1 + p^k x)^p &= 1 + \binom{p}{1} p^k x + \binom{p}{2} p^{2k} x^2 + \dots + \binom{p}{p-1} p^{(p-1)k} x^{p-1} + p^{pk} x^p \\ &= 1 + p^{k+1} \cdot \underbrace{\left(x + \binom{p}{2} p^{2k-(k+1)} x^2 + \dots + \binom{p}{p-1} p^{(p-1)k-(k+1)} x^{p-1} + p^{pk-(k+1)} x^p \right)}_y \end{aligned}$$

Since p divides those binomial coefficients, the expression y differs from x by a multiple of p . Looking at the very last term, $p^{pk-(k+1)} x^p$, we see that it is necessary that $pk - (k+1) \geq 1$ for this to work. Since all we know about k is that $k \geq 1$, it must be that $p > 2$ or this inequality could fail. This explains why the argument fails for the prime 2. So we have proven that

$$(1 + p^k x)^p = 1 + p^{k+1} y$$

with $y = x \pmod p$. Repeating this argument (that is, doing an induction), we get

$$(1 + p^k x)^{p^\ell} = 1 + p^{k+\ell} y$$

with $y = x \pmod p$. This is the formula asserted in the proposition.

Now let's see that this formula gives the assertion about orders. First we must see what the order in $\mathbf{Z}/p^{e \times}$ of elements of the form $1 + px$ can be. To do this we will invoke Lagrange's theorem. So we have to count the number of elements of $\mathbf{Z}/p^{e \times}$ expressible as $1 + px$. In the first place, for any integer x the integer $1 + px$ is relatively prime to p , so gives an element of $\mathbf{Z}/p^{e \times}$. On the other hand, if

$$1 + px = 1 + px' \pmod{p^e}$$

then $p^e \mid (1 + px - 1 - px')$. That is, $p^{e-1} \mid x - x'$. So the integers $1 + px$ and $1 + px'$ give the *same* element of $\mathbf{Z}/p^{e \times}$ only if $x = x' \pmod{p^{e-1}}$. Thus, the p^{e-1} integers $x = 0, 1, 2, \dots, p^{e-1} - 1$ give all the elements of $\mathbf{Z}/p^{e \times}$ expressible as $1 + px$.

By Lagrange's theorem, the order of any element $1 + px$ in $\mathbf{Z}/p^{e \times}$ must divide p^{e-1} .

This limitation allows our computation of $(1 + p^k x)^{p^\ell}$ to give a definitive answer to the question of order: for $p \nmid x$,

$$(1 + p^k x)^{p^\ell} = 1 + p^{k+\ell} y$$

with $y = x \pmod p$, so this is not $1 \pmod{p^e}$ unless $k + \ell \geq e$. (And if $k + \ell \geq e$ it is $1 \pmod{p^e}$.) Thus,

$$\text{(multiplicative) order of } 1 + p^k x \pmod{p^e} \text{ is } p^{e-k}$$

This proves the proposition. ♣

Proof: (of theorem and corollary) The assertion of the corollary is stronger than the theorem, so it certainly suffices to prove the more specific assertion of the corollary in order to prove the theorem.

Before the most serious part of the proof, let's see why an integer g which is a primitive root for \mathbf{Z}/p^e will also be a primitive root for $\mathbf{Z}/2p^{e \times}$. The main point is that for an odd prime p

$$\varphi(2p^e) = (2-1)(p-1)p^{e-1} = (p-1)p^{e-1} = \varphi(p^e)$$

Let g be a primitive root modulo p^e . Then $\ell = \varphi(p^e)$ is the smallest exponent so that $g^\ell = 1 \pmod{p^e}$. Thus, surely there is no *smaller* exponent ℓ so that $g^\ell = 1 \pmod{2p^e}$, since $p^e | 2p^e$. Therefore, a primitive root mod p^e also serves as a primitive root mod p^e .

Now the central case, that of primitive roots for \mathbf{Z}/p^e . That is, we want to show that the multiplicative group $\mathbf{Z}/p^{e \times}$ is of the form $\langle g \rangle$ for some g . Let g_1 be a primitive root mod p , which we already know exists for *other* reasons. The plan is to "adjust" g_1 suitably to obtain a primitive root mod p^e , somewhat in the spirit of Hensel's lemma. But it turns out that at most a single adjustment is necessary altogether, so in some regards the situation is *simpler* than a Hensel's lemma application.

If (by good luck?)

$$g_1^{p-1} = 1 + px$$

with $p \nmid x$, then let's show that g_1 is already a primitive root mod p^e for any $e \geq 1$. By Lagrange's theorem, the order of g_1 in $\mathbf{Z}/p^{e \times}$ is a divisor of $\varphi(p^e) = (p-1)p^{e-1}$. Since $p-1$ is the smallest positive exponent ℓ so that $g_1^\ell = 1 \pmod{p}$, $p-1$ divides the order of g_1 in $\mathbf{Z}/p^{e \times}$ (from our discussion of cyclic subgroups). Thus, the order of g_1 is in the list

$$p-1, (p-1)p, (p-1)p^2, \dots, (p-1)p^{e-1}$$

Thus, the question is to find the smallest positive ℓ so that

$$g_1^{(p-1)p^\ell} = 1 \pmod{p^e}$$

We are assuming that

$$g_1^{p-1} = 1 + px$$

with $p \nmid x$, so the question is to find the smallest positive ℓ so that

$$(1 + px)^{p^\ell} = 1 \pmod{p^e}$$

From the proposition, the smallest positive ℓ with this property is $\ell = e - 1$. That is, we have proven that g_1 is a primitive root mod p^e for *every* $e \geq 1$.

Now suppose that

$$g_1^{p-1} = 1 + px$$

with $p|x$. Then consider

$$g = (1 + p)g_1$$

Certainly g is still a primitive root mod p , because $g = g_1 \pmod{p}$. And we compute

$$\begin{aligned} (1+p)^{p-1} &= 1 + \binom{p-1}{1}p + \binom{p-1}{2}p^2 + \dots + \binom{p-1}{p-2}p^{p-2} + p^{p-1} \\ 1 + p \cdot \underbrace{\left(\binom{p-1}{1} + \binom{p-1}{2}p + \binom{p-1}{3}p^2 + \dots \right)}_y &= 1 + py \end{aligned}$$

Since

$$\binom{p-1}{1} = p-1$$

we see that

$$y = p-1 \pmod{p}$$

so $p \nmid y$. Thus,

$$g^{p-1} = ((1+p)g_1)^{p-1} = (1+py)(1+px) = 1 + p(y+x+pxy)$$

Since $p|x$, we have

$$y+x+pxy = y \pmod{p}$$

In particular, $p \nmid y+x+pxy$. Thus, by adjusting the primitive root a bit, we have returned to the first case above, that g^{p-1} is of the form $g^{p-1} = 1 + pz$ with $p \nmid z$. In that case we already saw that such g is a primitive root mod p^e for any $e \geq 1$.

This finishes the proof of existence of primitive roots in \mathbf{Z}/p^e for p an odd prime. ♣

20.3 Counting primitive roots

After proving *existence* of primitive roots, it is at least equally interesting to have an idea *how many* there are.

Theorem: If \mathbf{Z}/n has a primitive root, then there are exactly

$$\varphi(\varphi(n))$$

primitive roots mod n . (Yes, that is Euler's *phi* of Euler's *phi* of n .) For example, there are

$$\varphi(\varphi(p^e)) = \varphi(p-1) \cdot (p-1)p^{e-2}$$

primitive roots mod p^e for an odd prime p .

Proof: The hypothesis that \mathbf{Z}/n has a primitive root is that the multiplicative group \mathbf{Z}/n^\times is *cyclic*. That is, for some element g (the "primitive root")

$$\mathbf{Z}/n^\times = \langle g \rangle$$

Of course, the order $|g|$ of g must be the order $\varphi(n)$ of \mathbf{Z}/n^\times . From general discussion of cyclic subgroups, we know that

$$g^0, g^1, g^2, g^3, \dots, g^{\varphi(n)-1}$$

is a complete list of all the different elements of $\langle g \rangle$. And

$$\text{order of } g^k = \frac{\text{order of } g}{\gcd(k, |g|)}$$

So the generators for $\langle g \rangle$ are exactly the elements

$$g^k \text{ with } 1 \leq k < |g| \text{ and } k \text{ relatively prime to } |g|$$

By definition of Euler's φ -function, there are $\varphi(|g|)$ of these. Thus, since $|g| = \varphi(n)$, there are $\varphi(\varphi(n))$ primitive roots. ♣

Corollary: For an odd prime p , the fraction $\varphi(p-1)/p$ of the elements of \mathbf{Z}/p^{e^\times} consists of primitive roots.

Proof: From the theorem just proven the ratio of primitive roots to all elements is

$$\frac{\varphi(\varphi(p^e))}{\varphi(p^e)} = \frac{\varphi(p-1) \cdot (p-1)p^{e-2}}{(p-1)p^{e-1}} = \frac{\varphi(p-1)}{p}$$

as claimed. ♣

Remark: Thus, there are relatively *many* primitive roots modulo p^e .

20.4 Non-existence of primitive roots

For *generic* integers n , there is *no* primitive root in \mathbf{Z}/n .

Theorem: If n is *not* 4, 8, nor of the forms p^e , $2p^e$ for p an odd prime (and e a positive integer), then there is *no* primitive root modulo n .

Proof: First, let's look at $\mathbf{Z}/2^e$ with $e \geq 3$. Any $b \in \mathbf{Z}/2^{e \times}$ can be written as $b = 1 + 2x$ for integer x . Then

$$(1 + 2x)^2 = 1 + 4x + 4x^2 = 1 + 4x(x + 1)$$

The peculiar feature here is that for any integer x , the expression $x(x + 1)$ is divisible by 2. Indeed, if x is even surely $x(x + 1)$ is even, and if x is odd then $x + 1$ is even and $x(x + 1)$ is again even. Thus,

$$(1 + 2x)^2 = 1 \pmod{8}$$

(rather than merely modulo 4). And from the pattern

$$(1 + 2^k x)^2 = 1 + 2^{k+1} x + 2^{2k} x^2$$

we can prove by induction that

$$(1 + 8x)^{2^{e-3}} = 1 \pmod{2^e}$$

Putting this together, we see that

$$(1 + 2x)^{2^{e-2}} = 1 \pmod{2^e}$$

But $2^{e-2} < 2^{e-1} = \varphi(2^e)$. That is, there cannot be a primitive root modulo 2^e with $e > 2$.

Now consider n not a power of 2. Then write $n = p^e m$ with p an odd prime not dividing m . By Euler's theorem, we know that

$$b^{\varphi(p^e)} = 1 \pmod{p^e}$$

$$b^{\varphi(m)} = 1 \pmod{m}$$

Let $M = \text{lcm}(\varphi(p^e), \varphi(m))$. Then (as usual)

$$b^M = (b^{\varphi(p^e)})^{M/\varphi(p^e)} = 1^{M/\varphi(p^e)} = 1 \pmod{p^e}$$

and

$$b^M = (b^{\varphi(m)})^{M/\varphi(m)} = 1^{M/\varphi(m)} = 1 \pmod{m}$$

Thus, certainly

$$b^M = 1 \pmod{p^e m}$$

But a primitive root g would have the property that no smaller exponent ℓ than $\varphi(p^e m)$ has the property that $g^\ell = 1 \pmod{p^e m}$. Therefore, unless $\gcd(\varphi(p^e), \varphi(m)) = 1$ we'll have

$$\text{lcm}(\varphi(p^e), \varphi(m)) < \varphi(p^e) \varphi(m) = \varphi(p^e m)$$

which would deny the possibility that there be a primitive root.

Thus, we need $\varphi(m)$ relatively prime to $\varphi(p^e) = (p-1)p^{e-1}$. Since $p-1$ is even, this means that $\varphi(m)$ must be odd. If an odd prime q divides m , then $q-1$ divides $\varphi(m)$, which would make $\varphi(m)$ even, which is impossible. Thus, no odd prime can divide m . Further, if any power of 2 greater than just 2 itself divides m , again $\varphi(m)$ would be even, and no primitive root could exist.

Thus, except for the cases where we've already proven that a primitive root *does* exist, there is no primitive root mod n . ♣

#20.157 Find primitive roots modulo 11 and 13.

#20.158 Determine the order of all elements of the multiplicative groups $\mathbf{Z}/12^\times$, $\mathbf{Z}/15^\times$, $\mathbf{Z}/17^\times$.

21. Group Homomorphisms

- Group homomorphisms, isomorphisms
-

21.1 Group homomorphisms, isomorphisms

A *function* (or *map*)

$$f : G \rightarrow H$$

from one group G to another one H is a **group homomorphism** if

$$f(g_1 g_2) = f(g_1) f(g_2)$$

for all $g_1, g_2 \in G$. Let e_G be the identity in G and e_H the identity in H . The **kernel** of such a group homomorphism f is

$$\text{kernel of } f = \ker f = \{g \in G : f(g) = e_H\}$$

The **image** of f is just like the image of any function:

$$\text{image of } f = \text{im } f = \{h \in H : \text{there is } g \in G \text{ so that } f(g) = h\}$$

Let $f : G \rightarrow H$ be a group homomorphism. Let e_G be the identity in G and let e_H be the identity in H .

- Necessarily f carries the identity of G to the identity of H : $f(e_G) = e_H$.
- For $g \in G$, $f(g^{-1}) = f(g)^{-1}$.
- The *kernel* of f is a subgroup of G .
- The *image* of f is a subgroup of H .
- A group homomorphism $f : G \rightarrow H$ is *injective* if and only if the kernel is *trivial* (that is, is the trivial subgroup $\{e_G\}$).

Proof: The image $f(e_G)$ under f of the identity e_G in G has the property

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$$

using the property of the identity in G and the group homomorphism property. Left multiplying by $f(e_G)^{-1}$ (whatever this may be!), we get

$$f(e_G)^{-1} \cdot f(e_G) = f(e_G)^{-1} \cdot (f(e_G) \cdot f(e_G))$$

Simplifying and rearranging a bit, this is

$$e_H = (f(e_G)^{-1} \cdot f(e_G)) \cdot f(e_G) = e_H \cdot f(e_G) = f(e_G)$$

This proves that the identity in G is mapped to the identity in H .

To check that the image of an inverse is the image of an inverse, we simply compute

$$f(g^{-1}) \cdot f(g) = f(g^{-1} \cdot g)$$

by the homomorphism property, and this is

$$= f(e_G) = e_H$$

by the inverse property and by the fact (just proven) that the identity in G is mapped to the identity in H by a group homomorphism. Likewise, we also compute that

$$f(g) \cdot f(g^{-1}) = e_H$$

so the image of an inverse is the inverse of the image, as claimed.

To prove that the kernel of a group homomorphism $f : G \rightarrow H$ is a subgroup of G , we must prove three things. First, we must check that the identity lies in the kernel: this follows immediately from the fact just proven that $f(e_G) = e_H$. Next, we must show that if g is in the kernel then g^{-1} is also. Happily (by luck?) we just showed that $f(g^{-1}) = f(g)^{-1}$, so indeed if $f(g) = e_H$ then

$$f(g^{-1}) = f(g)^{-1} = e_H^{-1} = e_H$$

Finally, suppose both x, y are in the kernel of f . Then

$$f(xy) = f(x) \cdot f(y) = e_H \cdot e_H = e_H$$

so the “product” is also in the kernel.

Now let X be a subgroup of G . Let

$$f(X) = \{f(x) : x \in X\}$$

To show that $f(X)$ is a subgroup of H , we must check the usual three things: presence of the identity, closure under taking inverses, and closure under products. Again, we just showed that $f(e_G) = e_H$, so the image of a subgroup contains the identity. Also, we showed that $f(g)^{-1} = f(g^{-1})$, so the image of a subgroup is closed under inverses. And $f(xy) = f(x)f(y)$ by the defining property of a group homomorphism, so the image is closed under multiplication.

Finally, let’s prove that a homomorphism $f : G \rightarrow H$ is injective if and only if its kernel is trivial. First, if f is injective, then at most one element can be mapped to $e_H \in H$. Since we know that at least e_G is mapped to e_H by such a homomorphism, it must be that *only* e_G is mapped to e_H . Thus, the kernel is trivial.

On the other hand, suppose that the kernel is trivial. We will suppose that $f(x) = f(y)$, and show that $x = y$. Left multiply the equality $f(x) = f(y)$ by $f(x)^{-1}$ to obtain

$$e_H = f(x)^{-1} \cdot f(x) = f(x)^{-1} \cdot f(y)$$

By the homomorphism property, this gives

$$e_H = f(x)^{-1} \cdot f(y) = f(x^{-1}y)$$

Thus, $x^{-1}y$ is in the kernel of f , so (by assumption) $x^{-1}y = e_G$. Left multiplying this equality by x and simplifying, we get $y = x$. This proves the injectivity. ♣

If a group homomorphism $f : G \rightarrow H$ is *surjective*, then H is said to be a **homomorphic image** of G . If a group homomorphism $f : G \rightarrow H$ is a *bijection*, then f is said to be an **isomorphism**, and G and H are said to be **isomorphic**.

Remark: At least from a theoretical viewpoint, two groups that are *isomorphic* are considered to be “the same”, in the sense that any *intrinsic* group-theoretic assertion about one is also true of the other. In practical terms, however, the *transfer of structure* via the isomorphism may be difficult to *compute*.

#21.159 What is the kernel of the homomorphism

$$x \rightarrow x \bmod N$$

from \mathbf{Z} (with addition) to \mathbf{Z}/N (with addition modulo N)? (*Hint:* This may be easier than you think!)

#21.160 Let M, N be positive integers, and suppose that $N|M$. What is the kernel of the map

$$x \bmod M \rightarrow x \bmod N$$

from \mathbf{Z}/M (with addition modulo M) to \mathbf{Z}/N (with addition modulo N)?

#21.161 Let

$$\det : GL(2, \mathbf{Q}) \rightarrow \mathbf{Q}^\times$$

be the usual determinant map

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

Show by direct computation that \det is a group homomorphism.

#21.162 Show that the map

$$t \rightarrow \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

is an isomorphism from \mathbf{Q} (with addition) to a subgroup of $GL(2, \mathbf{Q})$.

#21.163 Show that the map

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \rightarrow a$$

is a *homomorphism* from the group of all matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ in which a, d are *non-zero* rational numbers and b is *any* rational number, to the multiplicative group \mathbf{Q}^\times of non-zero rational numbers. What is its kernel?

#21.164 Show that

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \rightarrow b$$

is *not* a homomorphism.

#21.165 Define a map $E : \mathbf{Q} \rightarrow GL(2, \mathbf{Q})$ by

$$x \rightarrow \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

Show that E is a group homomorphism from \mathbf{Q} with addition to a subgroup of $GL(2, \mathbf{Q})$.

#21.166 Define a map $E : \mathbf{Q} \rightarrow GL(3, \mathbf{Q})$ by

$$x \rightarrow \begin{pmatrix} 1 & x & \frac{x^2}{2} \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}$$

Show that E is a group homomorphism from \mathbf{Q} with addition to a subgroup of $GL(3, \mathbf{Q})$.

#21.167 Define a map $r : \mathbf{R} \rightarrow GL(2, \mathbf{R})$ by

$$x \rightarrow \begin{pmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{pmatrix}$$

Show that r is a group homomorphism from \mathbf{R} with addition to a subgroup of $GL(2, \mathbf{R})$. What is its kernel?

#21.168 Let n be an integer. Show that $f : \mathbf{Z} \rightarrow \mathbf{Z}$ defined by $f(x) = nx$ is a homomorphism.

#21.169 Show that a homomorphism $f : G \rightarrow H$ always has the property that $f(g^{-1}) = f(g)^{-1}$ for $g \in G$.

22. Cyclic Groups

- Finite cyclic groups
 - Infinite cyclic groups
 - Roots and powers
-

22.1 Finite cyclic groups

A finite group G is **cyclic** if there is $g \in G$ so that $\langle g \rangle = G$. And such a g is a **generator** of G , and G is said to be **generated by** g . (The case of *infinite* cyclic groups will be considered in the next section.)

Finite cyclic groups are the simplest of all groups, and can be readily understood as follows.

Let $N = |G|$. Since $G = \langle g \rangle$, also $N = |g|$. It is important to remember that (as proven a bit earlier)

- The elements $e = g^0, g^1, g^2, \dots, g^{N-2}, g^{N-1}$ form a complete list of the *distinct* elements of $G = \langle g \rangle$.
- With arbitrary integers i, j , we have $g^i = g^j$ if and only if $i \equiv j \pmod{N}$.
- Given an integer j , let i be the *reduction of* $j \pmod{N}$. Then $g^j = g^i$.

Then the collections of all *subgroups* and of all *generators* can be completely understood in terms of elementary arithmetic:

- The *distinct* subgroups of G are exactly the subgroups $\langle g^d \rangle$ for all *divisors* d of N .
- For $d|N$ the order of the subgroup $\langle g^d \rangle$ is the order of g^d , which is just N/d .
- The order of g^k with arbitrary integer $k \neq 0$ is $N/\gcd(k, N)$
- For any integer n we have

$$\langle g^n \rangle = \langle g^{gcd(n, N)} \rangle$$

- The distinct generators of G are the elements g^r where $1 \leq r < N$ and $gcd(r, N) = 1$. Thus, there are $\phi(N)$ of them, where ϕ is Euler's phi function.
- The number of elements of order n in a finite cyclic group of order N is 0 unless $n|N$, in which case it is N/n .

Remark: Some aspects of this can be paraphrased nicely in words: for example, *Every subgroup of a finite cyclic group is again a finite cyclic group, with order dividing the order of the group. Conversely, for every divisor of the order of the group, there is a **unique** subgroup of that order.*

Proof: Let's prove that the order of g^k is $N/\gcd(k, N)$. First, if $(g^k)^\ell = e = g^0$, then $k\ell \equiv 0 \pmod{N}$, from the simpler facts recalled above. That is, $N|k\ell$. That is, there is an integer m so that $k\ell = mN$. Then divide both sides of this equality by $\gcd(k, N)$, obtaining

$$\frac{k}{\gcd(k, N)} \cdot \ell = m \cdot \frac{N}{\gcd(k, N)}$$

Since now $N/\gcd(k, N)$ and $k/\gcd(k, N)$ are relatively prime, by unique factorization we conclude that

$$\frac{N}{\gcd(k, N)} \mid \ell$$

Therefore, the actual order of g^k is a multiple of $N/\gcd(k, N)$. On the other hand,

$$(g^k)^{N/\gcd(k, N)} = (g^N)^{k/\gcd(k, N)} = e^{k/\gcd(k, N)} = e$$

Note that we use the fact that $N/\gcd(k, N)$ and $k/\gcd(k, N)$ are both integers, so that all the expressions here have genuine content and sense. This finishes the proof that the order of g^k is $N/\gcd(k, N)$.

As a special case of the preceding, if $k \mid N$ then the order of g^k is $N/\gcd(k, N) = N/k$, as claimed above.

Since we know by now that $|\langle h \rangle| = |h|$ for any h , certainly

$$|\langle g^k \rangle| = |g^k| = N/\gcd(k, N)$$

Given integer k , let's show that

$$\langle g^k \rangle = \langle g^{\gcd(k, N)} \rangle$$

Let $d = \gcd(k, N)$, and let s, t be integers so that

$$d = sk + tN$$

Then

$$g^d = g^{sk+tN} = (g^k)^s \cdot (g^N)^t = (g^k)^s \cdot (e)^t = (g^k)^s \cdot e = (g^k)^s$$

so $g^d \in \langle g^k \rangle$. On the other hand,

$$g^k = (g^d)^{k/d}$$

since $d \mid k$. Thus, $g^k \in \langle g^d \rangle$. Therefore, since the subgroups $\langle g^k \rangle$ and $\langle g^d \rangle$ are closed under multiplication and under inverses, for any integer ℓ

$$(g^k)^\ell \in \langle g^d \rangle$$

and

$$(g^d)^\ell \in \langle g^k \rangle$$

But $\langle g^d \rangle$ is just the set of all integer powers of g^d (and similarly for g^k), so we have shown that

$$\langle g^d \rangle \subset \langle g^k \rangle$$

and vice-versa, so we find at last that

$$\langle g^d \rangle = \langle g^k \rangle$$

Therefore, all the *cyclic* subgroups of $\langle g \rangle = G$ are of the form $\langle g^d \rangle$ for some positive d dividing $N = |G| = |g|$. And different divisors d give different subgroups.

Let H be an *arbitrary* subgroup of G . We must show that H is generated by some g^k (so is in fact cyclic). Let k be the smallest positive integer so that $g^k \in H$. We claim that $\langle g^k \rangle = H$. For any other $g^m \in H$, we can write

$$m = q \cdot k + r$$

with $0 \leq r < k$. Then

$$g^r = g^{m-q \cdot k} = g^m \cdot (g^k)^{-q} \in H$$

since H is a subgroup. Since k was the smallest positive integer so that $g^k \in H$, and $0 \leq r < k$, it must be that $r = 0$. Therefore, m is a multiple of k , and g^k generates H .

As another particular case, notice that $\langle g^k \rangle = \langle g \rangle$ if and only if $\gcd(k, N) = 1$. And we may as well only consider $0 < k < N$, since otherwise we start repeating elements. That is, the distinct generators of $\langle g \rangle$ are the elements g^k with $0 < k < N$ and $\gcd(k, N) = 1$. So there certainly are $\varphi(N)$ of them.

Likewise, since

$$|g^k| = |\langle g^k \rangle| = |\langle g^{\gcd(k, N)} \rangle| = |g^{\gcd(k, N)}|$$

it is not hard to count the number of elements of a given order in $\langle g \rangle$. ♣

- A homomorphic image of a finite cyclic group is finite cyclic.

Proof: This follows by checking that the image of a generator is a generator for the image. ♣

- A finite cyclic group of order N is isomorphic to \mathbf{Z}/N . Specifically, for any choice of generator g of the cyclic group G , the map

$$f : n \rightarrow g^n$$

describes an isomorphism $f : \mathbf{Z}/N \rightarrow G$.

Proof: This is just a paraphrase of some of the other properties above.

A possibly disturbing issue here is that of proving that the map f as described above is **well-defined**. That is, we have some sort of formula which *appears* to describe a map, but there are hidden pitfalls. What we must show is that if $m = n \pmod N$ then $f(m) = f(n)$. (This has *nothing* to do with injectivity!) Well, it turns out that everything is ok, because we've already shown (in discussion of cyclic subgroups) that $g^m = g^n$ if and only if $m = n \pmod N$.

The crucial property which must be demonstrated is the homomorphism property

$$f(m + n) = f(m) \cdot f(n)$$

Indeed,

$$f(m + n) = f((m + n) \% N) = g^{(m+n) \% N} = g^{m+n}$$

since we proved (in the discussion of cyclic subgroups) that $g^i = g^j$ whenever $i = j \pmod N$. And then this is

$$= f(g^m) \cdot f(g^n)$$

as desired.

To see that f is injective, suppose that $f(m) = f(n)$ for integers m, n . Then $g^m = g^n$. Again, this implies that $m = n \pmod N$, which says that $m - \text{mod} - N = n - \text{mod} - N$, as desired. So f is injective.

The surjectivity is easy: given $g^n \in \langle g \rangle$, $f(n) = g^n$.

Therefore, the map f is a bijective homomorphism, so by definition is an isomorphism. ♣

22.2 Infinite cyclic groups

There are non-finite cyclic groups, as well, whose nature is also very simple, though somewhat different from the finite cyclic groups.

Dropping the assumption that a cyclic group is *finite* creates a few complications, but things are still tractable. And we can't overlook this possibility, since for example \mathbf{Z} with addition is an infinite cyclic group.

A group G is **infinite cyclic** if G is an *infinite* group and if there is $g \in G$ so that $\langle g \rangle = G$. Such a g is a **generator** of G , and G is said to be **generated by g** .

It is important to understand the assertions for *infinite* cyclic groups analogous to those for *finite* cyclic groups above:

- The elements $\dots, g^{-3}, g^{-2}, g^{-1}e = g^0, g = g^1, g^2, g^3, \dots$ are all *distinct* elements of $G = \langle g \rangle$.
- With integers i, j , we have $g^i = g^j$ if and only if $i = j$.

An *infinite cyclic group is isomorphic to \mathbf{Z}* . Specifically, for any choice of generator g of the infinite cyclic group G , the map

$$g^n \rightarrow n$$

describes an isomorphism $G \rightarrow \mathbf{Z}$. Thus, with hindsight, we realize that *an infinite cyclic group has just two generators*, since that is true of \mathbf{Z} .

Then the collections of all *subgroups* and of all *generators* can be completely understood in elementary terms:

- The *distinct* subgroups of G are exactly the subgroups $\langle g^d \rangle$ for all *non-negative* integers d .
- Any subgroup $\langle g^d \rangle$ is *infinite cyclic*, except for the trivial group $\{e\} = \{g^0\} = \langle g^0 \rangle$.
- Each subgroup $\langle g^d \rangle$ has exactly *two* generators, g^d and g^{-d} .

Some aspects of this can be paraphrased nicely in words: *Every non-trivial subgroup of an infinite cyclic group is again an infinite cyclic group*.

Also, about the number of elements of various orders: all elements of an infinite cyclic group are of infinite order except $e = g^0$, which is of order 1.

22.3 Roots, powers

In a cyclic group $G = \langle g \rangle$ of order n it is possible to reach very clear conclusions about the solvability of the equation $x^r = y$.

Let G be a cyclic group of order n with generator g . Fix an integer r , and define

$$f : G \rightarrow G$$

by

$$f(x) = x^r$$

Theorem: This map f is a group homomorphism of G to itself. If $\gcd(r, n) = 1$, then f is an *isomorphism*. That is, if $\gcd(r, n) = 1$, then every $y \in G$ has an r^{th} root, and has *exactly* one such root. Generally,

$$\text{order of kernel of } f = \gcd(r, n)$$

$$\text{order of image of } f = n/\gcd(r, n)$$

If an element y has an r^{th} root, then it has exactly $\gcd(r, n)$ of them. There are exactly $n/\gcd(r, n)$ r^{th} powers in G .

Proof: Certainly

$$\begin{aligned} f(x \cdot y) &= (xy)^r = x^r y^r \text{ (since } G \text{ is abelian)} \\ &= f(x) \cdot f(y) \end{aligned}$$

which shows that f is a homomorphism.

We may as well use the fact that G is isomorphic to \mathbf{Z}/n with addition (proven just above.) This allows us to directly use things we know about \mathbf{Z}/n and the relatively simple behavior of addition mod n to prove things about arbitrary finite cyclic groups. Thus, converting to the additive notation appropriate for \mathbf{Z}/n -with-addition, the map f is

$$f(x) = r \cdot x$$

We already know that if $\gcd(r, n) = 1$ then there is a multiplicative inverse r^{-1} to r mod n . Thus, the function

$$g(x) = r^{-1} \cdot x$$

gives an inverse function to f . This proves that f is both surjective and injective, so is a bijection, and thus an isomorphism.

For arbitrary r , let's look at the solvability of

$$r \cdot x = y \pmod{n}$$

for given y . Rewritten in more elementary terms, this is

$$n|(rx - y)$$

or, for some integer m ,

$$mn = rx - y$$

Let $d = \gcd(r, n)$. Then certainly it is *necessary* that $d|y$ or this equation is impossible. On the other hand, suppose that $d|y$. Write $y = dy'$ with some integer y' . Then we want to solve

$$r \cdot x = dy' \pmod{n}$$

“Dividing through” by the common divisor d , this congruence is equivalent to

$$\frac{r}{d} \cdot x = y' \pmod{\frac{n}{d}}$$

The removal of the common divisor has made r/d relatively prime to n/d , so there is a multiplicative inverse $(r/d)^{-1}$ to r/d mod n/d , and

$$x = (r/d)^{-1} \cdot y' \pmod{(n/d)}$$

That is, any integer x meeting this condition is a solution to the original congruence. Letting x_o be one such solution, the integers

$$x_o, x_o + \frac{n}{d}, x_o + 2 \cdot \frac{n}{d}, x_o + 3 \cdot \frac{n}{d}, \dots, x_o + (d-1) \cdot \frac{n}{d}$$

are also solutions, and are distinct mod n . That is, we have d distinct solutions mod n .

The necessary and sufficient condition $\gcd(r, n)|y$ for the equation $rx = y \pmod{n}$ to have a solution shows that there are exactly $n/\gcd(r, n)$ integers $y \pmod{n}$ which fulfill this condition. That is, there are exactly $n/\gcd(r, n)$ “ r^{th} powers”.

The kernel of f is the collection of x so that $rx = 0 \pmod{n}$. Taking out the common denominator $d = \gcd(r, n)$, this is $(r/d)x = 0 \pmod{n/d}$, which means $(n/d)|(r/d)x$. Since now r/d and n/d have no common factor, by unique factorization this implies that n/d divides x . Thus, mod n , there are d different solutions x . That is, the kernel of f has d elements. ♣

#22.170 List all elements of order 4 in $\mathbf{Z}/8$. List all elements of order 6 in $\mathbf{Z}/72$.

#22.171 Show that the subgroups $\langle 3 \rangle$ and $\langle 97 \rangle$ of $\mathbf{Z}/100$ generated by 3, 97 are the same subgroup.

#22.172 Suppose that $G = \langle g \rangle$ is a cyclic group of order 30. Compute the orders of the elements g^4 , g^8 , g^{12} , g^{16} , g^{20} , g^{24} , g^{28} .

#22.173 Suppose that G is a cyclic group, and has just 2 subgroups altogether: itself and the trivial subgroup $\{e\}$. What can you say about the order of G ?

#22.174 Suppose that G is a cyclic group, and has just 3 subgroups altogether: itself, the trivial subgroup $\{e\}$, and a (*proper*) subgroup of order 13. What is the order of G ?

#22.175 Prove that for any subgroup H of \mathbf{Z} other than the trivial subgroup $\{0\}$ the *smallest positive element* s of H is a generator for H , which is a cyclic group.

#22.176 Let g, h be elements of a group G , and $|g| = 30$ while $|h| = 77$. Show that $\langle g \rangle \cap \langle h \rangle = \{e\}$.

#22.177 Let p be a prime. Suppose that a group G has p elements. Prove that G is *cyclic*. (*Hint*: take $g \neq e$ and look at $\langle g \rangle$: use Lagrange's theorem).

#22.178 Let m, n be relatively prime. Let H, K be subgroups of a group G where $|H| = m$ and $|K| = n$. Show that $H \cap K = \{e\}$.

#22.179 Let p be a prime congruent to 3 modulo 4. Suppose that a is a square in \mathbf{Z}/p . Show that $a^{(p+1)/4}$ is a square root of a .

#22.180 Let p be a prime congruent to 7 mod 9. If a is a cube in \mathbf{Z}/p , show that $a^{(p+2)/9}$ is a cube root of a .

#22.181 Let p be a prime congruent to 4 mod 9. If a is a cube in \mathbf{Z}/p , show that $a^{(p+5)/9}$ is a cube root of a .

23. (*) Carmichael numbers and witnesses

At last we are in a position to prove that our probabilistic primality tests really work.

- Exponent of \mathbf{Z}/n^\times : Carmichael's lambda
- Simple properties of Carmichael numbers
- Euler (Solovay-Strassen) witnesses
- Strong (Miller-Rabin) witnesses

23.1 Exponent of \mathbf{Z}/n^\times : Carmichael's lambda

To understand Carmichael numbers means to understand how the Fermat pseudoprime test fails. To understand this mechanism we continue in the spirit of Euler's theorem and Fermat's Little Theorem.

For a positive integer n , define Carmichael's **lambda function**

$$\lambda(n) = \text{exponent of the multiplicative group } \mathbf{Z}/n^\times$$

This usage is consistent with the notion of *exponent* of an arbitrary group G . That is, $\lambda(n)$ is the *least* positive integer so that for every $x \in \mathbf{Z}/n^\times$

$$x^{\lambda(n)} = 1 \pmod n$$

We already know (from discussion of cyclic subgroups) that if $x^k = 1 \pmod n$ then the order $|x|$ of x divides k : to recall how the proof of this important fact goes, write $k = q \cdot |x| + r$ with $0 \leq r < |x|$. Then

$$1 = x^k = x^{q \cdot |x| + r} = (x^{|x|})^q \cdot x^r = (1)^q \cdot x^r = x^r \pmod n$$

Since $|x|$ is the smallest *positive* integer so that $x^{|x|} = 1 \pmod n$, it must be that $r = 0$, so $|x|$ indeed divides n .

We also know, from Lagrange's theorem, that the exponent of a finite group divides the order of the group. Thus,

$$\lambda(n) = \text{exponent of } \mathbf{Z}/n^\times \text{ divides } \varphi(n)$$

Now we can completely determine $\lambda(n)$. It is *not* weakly multiplicative, but nevertheless behaves in a way that is manageable.

Theorem:

- For m and n relatively prime, the Carmichael lambda function has the property

$$\lambda(m \cdot n) = \text{lcm}(\lambda(m), \lambda(n))$$

- For an odd prime p , $\lambda(p^e) = \varphi(p^e) = (p - 1)p^{e-1}$. Since there is a primitive root mod p^e , there is an element whose order is $\lambda(p^e)$.
- For powers of 2: $\lambda(2) = 1$, $\lambda(4) = 2$, and $\lambda(2^e) = 2^{e-2}$ for $e > 2$. There is an element of $\mathbf{Z}/2^{e \times}$ whose order is $\lambda(2^e)$.

Proof: For m and n relatively prime, by Sun Ze's theorem the system

$$x^k = 1 \pmod{m} \quad x^k = 1 \pmod{n}$$

is equivalent to the single congruence

$$x^k = 1 \pmod{mn}$$

Thus, if $x^k = 1 \pmod{mn}$ certainly $x^k = 1 \pmod{m}$ and $x^k = 1 \pmod{n}$. Thus, by the observation just before the statement of the theorem, certainly $\lambda(m)$ and $\lambda(n)$ both divide $\lambda(mn)$. Thus, $\lambda(mn)$ is a common multiple of the two. On the other hand, let M be any common multiple of $\lambda(m)$ and $\lambda(n)$. Write $M = m'\lambda(m)$ and $M = n'\lambda(n)$ for some integers m' and n' . Then

$$x^M = (x^{\lambda(m)})^{m'} = 1^{m'} = 1 \pmod{m}$$

and

$$x^M = (x^{\lambda(n)})^{n'} = 1^{n'} = 1 \pmod{n}$$

Thus, by Sun Ze (using the relative prime-ness of m and n)

$$x^M = 1 \pmod{mn}$$

That is, if M is divisible by all the orders mod m and by all the orders mod n , it is divisible by all the orders mod mn . This proves that

$$\lambda(m \cdot n) = \text{lcm}(\lambda(m), \lambda(n))$$

For p an odd prime we know that there is a primitive root g modulo p^e . Thus, there is an element of order $(p - 1)p^{e-1} = \varphi(p^e)$ in $\mathbf{Z}/p^{e \times}$. Thus, $\varphi(p^e)$ divides $\lambda(p^e)$. By Lagrange's theorem, the order of *any* element in $\mathbf{Z}/p^{e \times}$ divides the order $\varphi(p^e)$ of $\mathbf{Z}/p^{e \times}$. Thus, thinking again of the observation just before the theorem, $\lambda(p^e) = \varphi(p^e)$.

Now consider powers of 2. The group $\mathbf{Z}/2^\times$ has just one element, so its order is necessarily 1. The group $\mathbf{Z}/4^\times$ has order 2, so necessarily has order 2.

In showing that there is *no* primitive root mod 2^e for $e \geq 3$, we already noted that

$$(1 + 2x)^2 = 1 + 4x(1 + x) = 1 \pmod{8}$$

for any integer x . And, further, we saw that

$$(1 + 8x)^{2^k} = 1 \pmod{2^{3+k}}$$

Therefore,

$$(1 + 2x)^{2^{e-2}} = 1 \pmod{2^e}$$

for $e \geq 3$. Thus, the actual order of any element must be a divisor of 2^{e-2} . On the other hand, for $k \geq 2$, and for odd integer x ,

$$(1 + 2^k x)^2 = 1 + 2^{k+1} x + 2^{2k} x^2 = 1 + 2^{k+1} \cdot \underbrace{(x + 2^{k-1} x^2)}_y = 1 + 2^{k+1} y$$

Since $k \geq 2$, $2^{k-1} x^2$ is even, so $y = x \pmod 2$. Thus, by induction,

$$(1 + 4x)^{2^\ell} = 1 + 2^{2+\ell} y$$

with $y = x \pmod 2$. In particular, this is not $1 \pmod{2^e}$ unless $2 + \ell \geq e$. Thus, for example, the element $1 + 4$ has order 2^{e-2} in $\mathbf{Z}/2^{e \times}$. Thus,

$$\lambda(2^e) = 2^{e-2} \text{ for } e \geq 3$$

This completes the computation of $\lambda(n)$. ♣

23.2 Simple properties of Carmichael numbers

Even though it is awkward that there are infinitely-many Carmichael numbers, there are demonstrable restrictions on what kind of numbers may be Carmichael. These restrictions are used in proving that the more refined Solovay-Strassen and Miller-Rabin tests (probabilistically) *succeed* in detecting compositeness.

Theorem: A positive integer is a Carmichael number if and only if

$$\lambda(n) \text{ divides } n - 1$$

In particular, a Carmichael number is necessarily odd, square-free, and divisible by at least three different primes.

Proof: Suppose n is Carmichael. That is, suppose that for every b relatively prime to n we have

$$b^{n-1} = 1 \pmod n$$

By definition, the Carmichael function $\lambda(n)$ gives the smallest positive integer so that

$$b^{\lambda(n)} = 1 \pmod n$$

for all b prime to n . We have seen that there exists an element whose order is exactly $\lambda(n)$. Let b be such an element. Write $n - 1 = q \cdot \lambda(n) + r$ with $0 \leq r < \lambda(n)$. Then

$$1 = b^{n-1} = b^{q \cdot \lambda(n) + r} = (b^{\lambda(n)})^q \cdot b^r \pmod n$$

Since $\lambda(n)$ is the least positive integer so that b raised to that power is 1 modulo n , it must be that $r = 0$, so $\lambda(n)$ divides $n - 1$. From this fact the other particular assertions will follow.

From the general formula for $\lambda(n)$, notice that if $n > 2$ then 2 divides $\lambda(n)$: if n has any prime p factor other than 2, then $p - 1$ divides $\lambda(n)$. On the other hand, if n is a power of 2 larger than 2 itself, then for 2 divides $\lambda(n)$.

Therefore, if n is Carmichael, then since 2 divides $\lambda(n)$ and (as we just saw) $\lambda(n)$ divides $n - 1$, it must be that 2 divides $n - 1$. Thus, n is odd.

If for some odd prime p a power p^e divides n with $e > 1$, then p divides $\lambda(n)$. Since $\lambda(n)$ divides $n - 1$, this implies that p divides $n - 1$. But this can't happen when p divides n . Thus, n is square-free.

If n is just the product $n = pq$ of two different odd primes p, q , then

$$\lambda(n) = \lambda(pq) = \text{lcm}(\lambda(p), \lambda(q)) = \text{lcm}(p - 1, q - 1)$$

And $\lambda(n)$ divides $n - 1 = pq - 1$, so we obtain

$$p - 1 \mid pq - 1$$

and

$$q - 1 \mid pq - 1$$

We can rearrange a little:

$$p - 1 \text{ divides } pq - 1 = (p - 1)q + q - 1$$

Therefore, $p - 1$ divides $q - 1$. Symmetrically, $q - 1$ divides $p - 1$. But since $p \neq q$ this is impossible. Thus, n must be divisible by at least three different primes. ♣

23.3 Euler (Solovay-Strassen) witnesses

Now we prove the *existence* of Euler witnesses to the compositeness of non-prime numbers, in contrast to the fact that Carmichael numbers have no *Fermat* witnesses to their compositeness. Also we prove that there are *many* Euler witnesses for composite numbers, in the sense that at least half the numbers b in the range $1 < b < n$ are Euler witnesses to the compositeness of n .

Proposition: An Euler witness to the primality of n is also a Fermat witness to the primality of n . In the other direction, a Fermat witness to the compositeness of n is an Euler witness to the compositeness. In other words, a *false* Euler witness to primality is a *false* Fermat witness to primality. In particular, if there were a composite number n with no Euler witnesses to its compositeness, then n would have to be a Carmichael number.

Proof: What we assert is that if

$$b^{(n-1)/2} = \left(\frac{b}{n}\right)_2 \pmod{n}$$

for b relatively prime to n , then

$$b^{n-1} = 1 \pmod{n}$$

Indeed, squaring both sides of the first equation, we get

$$b^{n-1} = \left(\frac{b}{n}\right)_2^2 \pmod{n}$$

Since b is relatively prime to n , the quadratic symbol has value ± 1 , so its square is unavoidably just 1. Thus, the Euler witness b is certainly a Fermat witness.

So if n were a composite number so that nevertheless for all b relatively prime to n

$$b^{(n-1)/2} = \left(\frac{b}{n}\right)_2 \pmod{n}$$

then also $b^{n-1} = 1 \pmod{n}$ for all such b , and n is Carmichael. ♣

Remark: Thus, we might say

$$\{ \text{Euler pseudoprimes} \} \subset \{ \text{Fermat pseudoprimes} \}$$

Or, more precisely,

$$\{ \text{Euler pseudoprimes base } b \} \subset \{ \text{Fermat pseudoprimes base } b \}$$

Now we prove existence of Euler witnesses to compositeness:

Theorem: Existence of Euler witnesses: Assume that n is a positive composite integer. Then there is at least one integer b in the range $1 < b < n$ and with $\gcd(b, n) = 1$ so that

$$b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right)_2$$

That is, there exists an Euler witness.

Proof: If n is not Carmichael, then there is already a Fermat witness b to the compositeness of n , so b is certainly an Euler witness.

So consider a Carmichael number n . From above, this implies that n is square-free and odd. So write $n = pm$ with p prime and p not dividing m . Let b_o be a quadratic non-residue mod p , and (by Sun Ze) find b so that $b \equiv b_o \pmod{p}$ and $b \equiv 1 \pmod{m}$. Then, on one hand,

$$\left(\frac{b}{n}\right)_2 = \left(\frac{b}{pm}\right)_2 = \left(\frac{b}{p}\right)_2 \left(\frac{b}{m}\right)_2 = \left(\frac{b_o}{p}\right)_2 \left(\frac{1}{m}\right)_2 = (-1)(+1) = -1$$

using the definition

$$\left(\frac{b}{pm}\right)_2 = \left(\frac{b}{p}\right)_2 \left(\frac{b}{m}\right)_2$$

of the Jacobi symbol for composite lower input. On the other hand,

$$b^{(n-1)/2} \equiv 1^{(n-1)/2} \equiv 1 \pmod{m}$$

so already modulo m we have

$$b^{(n-1)/2} \not\equiv \left(\frac{b}{pm}\right)_2 \pmod{m}$$

which surely gives

$$b^{(n-1)/2} \not\equiv \left(\frac{b}{pm}\right)_2 \pmod{pm}$$

Therefore, this b is an Euler witness to the compositeness of $n = pm$. ♣

Now, invoking Lagrange's theorem, we can prove that there are "many" Euler witnesses:

Corollary: For composite n , at least half the numbers b in the range $1 < b < n$ are Euler witnesses to the compositeness of n .

Proof: The idea is to show that the collection L of false witnesses (but relatively prime to n) is a *subgroup* of \mathbf{Z}/n^\times . Since (by the theorem) there is at least *one* witness, the subgroup of *false* witnesses is a *proper* subgroup. By Lagrange's theorem, the order $|L|$ of L must be a *proper* divisor of the order $\varphi(n)$ of \mathbf{Z}/n^\times . Therefore, certainly

$$|L| \leq \frac{1}{2}\varphi(n) \leq \frac{1}{2}(n-1)$$

So let's prove that the collection L of witnesses to the primality of n is a subgroup of \mathbf{Z}/n^\times . Suppose that x, y are witnesses to the primality of n . That is,

$$x^{(n-1)/2} = \left(\frac{x}{n}\right)_2 \pmod n$$

and

$$y^{(n-1)/2} = \left(\frac{y}{n}\right)_2 \pmod n$$

Then

$$(xy)^{(n-1)/2} = x^{(n-1)/2} \cdot y^{(n-1)/2} = \left(\frac{x}{n}\right)_2 \cdot \left(\frac{y}{n}\right)_2 \pmod n$$

We know that

$$\left(\frac{x}{n}\right)_2 \cdot \left(\frac{y}{n}\right)_2 = \left(\frac{xy}{n}\right)_2$$

Thus,

$$(xy)^{(n-1)/2} = x^{(n-1)/2} \cdot y^{(n-1)/2} = \left(\frac{x}{n}\right)_2 \cdot \left(\frac{y}{n}\right)_2 = \left(\frac{xy}{n}\right)_2 \pmod n$$

Thus, xy is again a witness to the primality of n .

Next, we check that the (multiplicative) identity 1 in \mathbf{Z}/n^\times is in L . This is silly:

$$1^{(n-1)/2} = 1 = \left(\frac{1}{n}\right)_2 \pmod n$$

Next, we check that the set L of witnesses is closed under taking multiplicative inverses modulo n . Let $x \in L$, and let x^{-1} denote its inverse modulo n . First, we have

$$\left(\frac{x}{n}\right)_2 \cdot \left(\frac{x^{-1}}{n}\right)_2 = \left(\frac{x \cdot x^{-1}}{n}\right)_2 = \left(\frac{1}{n}\right)_2 = 1$$

Thus,

$$\left(\frac{x^{-1}}{n}\right)_2 \left(\frac{x}{n}\right)_2 = 1$$

Then, using properties of exponents,

$$(x^{-1})^{(n-1)/2} = (x^{(n-1)/2})^{-1} = \left(\frac{x}{n}\right)_2^{-1} = \left(\frac{x^{-1}}{n}\right)_2 \pmod n$$

That is, if x is a witness then so is x^{-1} .

Thus, L is closed under multiplication, closed under inverses, and contains the identity, so is a subgroup of \mathbf{Z}/n^\times . Since we showed that for composite n there is at least one b which is *not* a (false!) witness to the primality of n , for composite n the subgroup of (false!) witnesses is a *proper subgroup*. Thus, as indicated at the beginning of the proof, by Lagrange's theorem we conclude that at least half of the numbers in the range $1 < b < n$ will detect the compositeness of composite n . ♣

Thus, we are assured that the Solovay-Strassen primality test "works".

23.4 Strong (Miller-Rabin) witnesses

Now we prove that there are strong witnesses, and that in fact for odd composite n at least $3/4$ of the numbers in the range $1 < b < n$ are witnesses to the compositeness of n . Thus, the Miller-Rabin test “works”. Along the way, we compare strong pseudoprimes and Euler pseudoprimes.

Let n be a fixed odd integer throughout this discussion, and let $n - 1 = 2^s \cdot m$ with m odd. Since n is odd, $s \geq 1$.

Let’s review the Miller-Rabin test, using a *single* auxiliary number b . First, choose a “random” auxiliary number b from the range $1 < b < n$, and compute $c = b^m$. If $c = 1 \pmod n$, then stop: b is a **strong witness** to the primality of n . If c is not $-1 \pmod n$, then start computing successive squares:

$$c^2, c^4 = (c^2)^2, c^8 = ((c^2)^2)^2, c^{2^4} = (c^8)^2, \dots, c^{2^{s-1}}$$

If for any $k < s$ we obtain $c^{2^k} = -1 \pmod n$, then stop: b is a **strong witness** to the primality of n . On the other hand, if for some k we obtain $c^{2^k} = 1 \pmod n$ but $c^{2^{k-1}} \neq -1 \pmod n$, then n is **definitely composite**. And, if no $c^{2^k} = 1$, for $0 \leq k \leq s$, then n is **definitely composite**.

Remark: If no $c^{2^k} = 1$, for $0 \leq k \leq s$, then $b^{n-1} \neq 1 \pmod n$, so already n fails the Fermat pseudoprime base b test.

If auxiliary numbers b_1, b_2, \dots, b_k are used, and if each is a witness to the primality of n , then we imagine that n is prime with “probability”

$$1 - \left(\frac{1}{4}\right)^k$$

We should verify that a genuine prime is a strong pseudoprime for any base b . That is, we should verify that a genuine prime will pass any number of rounds of the Miller-Rabin test.

Proposition: Genuine primes are strong pseudoprimes, and pass the Miller-Rabin test. That is: let $p > 2$ be prime, and $p - 1 = 2^s \cdot m$ with m odd. Let b be any integer not divisible by p . Let t be the smallest non-negative integer so that $(b^m)^{2^t} = 1 \pmod p$. Then either $t = 0$, or

$$(b^m)^{2^{t-1}} = -1 \pmod p$$

Proof: Since p is prime, \mathbf{Z}/p is a *field*, and by the Fundamental Theorem of Algebra, the equation $x^2 - 1 = 0$ has number of roots at most equal to its degree. Thus, $\pm 1 \pmod p$ are the only elements of \mathbf{Z}/p whose square is $1 \pmod p$. Thus, if $(b^m)^{2^t} = 1 \pmod p$ but $(b^m)^{2^{t-1}} \neq 1 \pmod p$, the only possibility is that $(b^m)^{2^{t-1}} = -1 \pmod p$. Thus, the genuine prime p would pass every such test. ♣

Now we have a simple argument to show that the Miller-Rabin test is at least as discriminating as the Fermat test. This fact is also a corollary of the fact (already proven) that Euler witnesses are Fermat witnesses, together with the fact (proven below) that strong witnesses are Euler witnesses. But this proposition itself has a much simpler proof:

Proposition: A strong witness to the primality of n is also a Fermat witness.

Proof: Let b the random number chosen, and let $c = b^m$. First suppose that $c = 1$. Then

$$b^{n-1} = b^{m \cdot 2^s} = c^{2^s} = 1^{2^s} = 1 \pmod n$$

so b is a Fermat witness. Or, if

$$c^{2^t} = -1 \pmod n$$

with $t < s$, then

$$b^{n-1} = b^{m \cdot 2^s} = c^{2^s} = (c^{2^t})^{2^{s-t}} = (-1)^{2^{s-t}} = 1 \pmod{n}$$

So again in this case b is a Fermat witness. ♣

Before proving that strong witnesses are Euler witnesses, we need some notation, and a preliminary computation: for positive integer N and an integer k , let

$$\text{ord}_N k = \text{order of } k \text{ in the multiplicative group } \mathbf{Z}/N^\times$$

Lemma: For integer k and an odd prime p (not dividing k),

$$\text{ord}_{p^e} k / \text{ord}_p k = \text{non-negative power of } p$$

Proof: We use the fact that $\mathbf{Z}/p^{e \times}$ is a cyclic group, that is, that there is a primitive root g . Let ℓ be a positive integer so that $g^\ell = k$. From the discussion of cyclic groups and cyclic subgroups,

$$\text{ord}_{p^e} k = \varphi(p^e) / \gcd(\ell, \varphi(p^e))$$

$$\text{ord}_p k = \varphi(p) / \gcd(\ell, \varphi(p))$$

Since $p-1$ and p^{e-1} are relatively prime,

$$\gcd(\ell, \varphi(p^e)) = \gcd(\ell, (p-1)p^{e-1}) = \gcd(\ell, p-1) \cdot \gcd(\ell, p^{e-1})$$

Thus,

$$\begin{aligned} \text{ord}_{p^e} k / \text{ord}_p k &= \frac{\varphi(p^e) / \gcd(\ell, \varphi(p^e))}{\varphi(p) / \gcd(\ell, \varphi(p))} = \frac{(p-1)p^{e-1} \cdot \gcd(\ell, \varphi(p))}{(p-1) \cdot \gcd(\ell, \varphi(p^e))} \\ &= \frac{p^{e-1}}{\gcd(\ell, p^{e-1})} \end{aligned}$$

This proves the assertion. ♣

Theorem: A strong witness to the primality of n is also an Euler witness.

Proof: First, if n is prime then it will pass any number of rounds of either Solovay-Strassen or Miller-Rabin tests.

So consider composite odd n . Let b the random number chosen, and let $c = b^m$. Let the prime factorization of n be

$$n = p_1^{e_1} \dots p_N^{e_N}$$

let b be a strong witness for n , and put $c = b^d$. The hypothesis that b is a strong witness for n is that either

$$(i) \ c = 1 \pmod{n}$$

or

$$(ii) \ c^{2^t} = -1 \pmod{n} \text{ for some } 1 \leq t < s$$

Since $c^{2^t} = -1 \pmod{p^e}$ for each prime power p^e dividing n ,

$$\text{ord}_{p^e} c = 2^{t+1}$$

and, therefore,

$$\text{ord}_{p^e} b = 2^{t+1} \times (\text{odd})$$

(In the case that $c = 1$, these orders are odd, and 2^0 divides them, etc.)

By the lemma, also

$$\text{ord}_p b = 2^{t+1} \times (\text{odd})$$

since the only thing that might change is the power of p occurring.

Let 2^{t_i} be the exact power of 2 dividing $p_i - 1$. Thus,

$$t + 1 \leq k_i \text{ for all } i$$

Let g_i be a primitive root mod p_i , and write $b = g_i^{\ell_i}$ with $\ell_i | p_i - 1$. Then (from discussion of cyclic subgroups)

$$\text{ord}_{p_i} b = \frac{p_i - 1}{\ell_i}$$

Thus, for a given index i , if $t + 1 < k_i$, then b is a square mod p_i . It is only for $t + 1 = k_i$ that b is a non-square mod p_i .

Let M be the number of indices i so that b is a non-square mod p_i , and so that $t + 1 = k_i$. Then

$$\left(\frac{b}{n}\right)_2 = \left(\frac{b}{p_1}\right)_2^{e_1} \cdots \left(\frac{b}{p_N}\right)_2^{e_N} = (-1)^M$$

On the other hand, since $2^{t+1} | p_i - 1$ for each index i , write

$$p_i = 1 + 2^{t+1} x_i$$

for some odd number x_i . Then

$$p_i^2 = 1 + 2 \cdot 2^{t+1} x_i + 2^{2t+2} x_i^2 = 1 \pmod{2^{t+2}}$$

Thus, modulo 2^{t+2} , all the prime powers in n with exponent 2 or higher are just 1. And, modulo 2^{t+2} ,

$$p_i = 1 + 2^{t+1} \cdot (\text{odd}) \equiv 1 + 2^{t+1} \pmod{2^{t+2}}$$

Thus, the prime powers occurring in n with exponent just 1 contribute factors of $1 + 2^{t+1}$ modulo 2^{t+2} . Therefore, modulo 2^{t+2} ,

$$\begin{aligned} n &= p_1^{e_1} \cdots p_N^{e_N} = (1 + 2^{t+1})^M \pmod{2^{t+2}} \\ &= 1 + \binom{M}{1} 2^{t+1} + \binom{M}{2} 2^{2t+2} + \binom{M}{3} 2^{3t+3} + \cdots = 1 + M \cdot 2^{t+1} \pmod{2^{t+2}} \end{aligned}$$

Thus, depending upon whether M is odd or even:

$$n = 1 + M \cdot 2^{t+1} = 1 + 2^{t+1} \pmod{2^{t+2}} \text{ (for } M \text{ odd)}$$

$$n = 1 + M \cdot 2^{t+1} = 1 \pmod{2^{t+2}} \text{ (for } M \text{ even)}$$

Therefore, in the case that M is odd, the power of 2 dividing $n - 1$ is *exactly* 2^{t+1} . That is, $s = t + 1$. Therefore,

$$b^{(n-1)/2} = b^{m \cdot 2^{s-1}} = c^{2^{s-1}} = c^{2^t} = -1 \pmod{n}$$

So for M odd, we have

$$b^{(n-1)/2} = -1 = \left(\frac{b}{n}\right)_2$$

And, therefore, in the case that M is even, the power of 2 dividing $n - 1$ is *at least* 2^{t+2} . That is, $s \geq t + 2$. Therefore,

$$b^{(n-1)/2} = b^{m \cdot 2^{s-1}} = c^{2^{s-1}} = (c^{2^t})^{2^{s-1-2^t}} = (-1)^{2^{s-1-2^t}} = 1 \pmod n$$

So once again we have

$$b^{(n-1)/2} = 1 = \left(\frac{b}{n}\right)_2$$

This completes the proof that strong witnesses are Euler witnesses. ♣

Theorem: If an odd integer n is composite, then at least $3/4$ of the integers b in the range $1 < b < n$ are strong (Miller-Rabin) witnesses to the compositeness of n .

Proof: Let k be the largest non-negative integer so that there is at least one b with $b^{2^k} = -1 \pmod n$. Since $(-1)^{2^0} = -1$, there exists such k .

Lemma: $n \equiv 1 \pmod{2^{k+1}}$

Proof: (of lemma) With $b^{2^k} = -1 \pmod n$, certainly $b^{2^{k+1}} = 1 \pmod n$. Thus, $n | b^{2^{k+1}} - 1$. Thus, by Fermat's observation, for any prime p dividing n , either $p | b^{2^\ell} - 1$ for some $\ell < k + 1$, or $p = 1 \pmod{2^{k+1}}$. Since by hypothesis $b^{2^k} = -1 \pmod n$ and b^{2^r} is neither $1 \pmod n$ nor $-1 \pmod n$ for $r < k$, it cannot be that $p | b^{2^\ell} - 1$ for some $\ell < k + 1$. Thus, for any prime p dividing n we have $p = 1 \pmod{2^{k+1}}$. Multiplying any number of such primes together gives a product n which must also be $1 \pmod{2^{k+1}}$. ♣

Now return to the proof of the theorem. Let $\ell = 2^k \cdot m$, with $n - 1 = 2^s \cdot m$ and m odd, as above. By the lemma, $2\ell | n - 1$. Define subgroups of $G = \mathbf{Z}/n^\times$:

$$\begin{aligned} H &= \{g \in G : a^{n-1} = 1 \pmod n\} \\ I &= \{g \in G : g^\ell = \pm 1 \pmod{p_i^{e_i}} \text{ for all } i\} \\ J &= \{g \in G : g^\ell = \pm 1 \pmod n\} \supset \{ \text{strong liars} \} \\ K &= \{g \in G : a^\ell = 1 \pmod n\} \end{aligned}$$

It is not so hard to check that we have inclusions

$$G \supset H \supset I \supset J \supset K$$

(It is very easy to check, from the definition of subgroup, that all these are subgroups of G .)

Lemma: The *strong liars* (false witnesses to the primality of n) all lie in J .

Proof: (of Lemma) First, if $b^m = 1 \pmod n$, then surely $b^\ell = 1 \pmod n$, since $m | \ell$. On the other hand, if

$$b^{m \cdot 2^t} = -1 \pmod n$$

for some $t < s$, then $t \leq k$ by the definition of k . Thus,

$$b^\ell = b^{m \cdot 2^k} = (b^{m \cdot 2^t})^{2^{k-t}} = (-1)^{2^{k-t}} \pmod n$$

Thus, indeed, any strong liar is in J . ♣

Next, except for the special case $n = 9$ which is easy to dispatch directly, we'll show that

$$[G : J] \geq 4$$

Since the strong liars are contained in J , this will show that

$$\text{number of witnesses to compositeness of } n \geq (n-1) - \frac{1}{4}\varphi(n) \geq (n-1) - \frac{1}{4}(n-1) = \frac{3}{4}(n-1)$$

as desired.

Let

$$f : G \rightarrow G$$

be the map

$$f(g) = g^\ell$$

Since G is abelian, this is a group homomorphism.

Lemma: Let

$$S = \{a \in G : a = \pm 1 \pmod{p_i^{e_i}} \text{ for all indices } i\}$$

Every element of S is a $(2^k)^{\text{th}}$ power of some element in G . Therefore, every element of S is an ℓ^{th} power of some element in G . That is, the group homomorphism $f : G \rightarrow S$ is a *surjection*.

Proof: (of Lemma) Let x be an integer so that $x = b \pmod{p_i^{e_i}}$ or $x = b^2 \pmod{p_i^{e_i}}$, with possibly different choices for different primes p_i , where b is the special element as above. Then $x^{2^k} = +1 \pmod{p_i^{e_i}}$ if $x = b^2 \pmod{p_i^{e_i}}$, and $x^{2^k} = -1 \pmod{p_i^{e_i}}$ if $x = b \pmod{p_i^{e_i}}$. This proves the first assertion of the lemma.

Since m is odd, both $\pm 1 \pmod{p_i^{e_i}}$ are m^{th} powers of themselves. Thus, if

$$g^{2^k} = h$$

with $h \in S$ then

$$g^\ell = g^{2^k \cdot m} = h^m = h \pmod{p_i^{e_i}}$$

for all indices i . This proves that f is surjective. ♣

We want to claim that K has index 2^N in I . We can get this as a corollary of a lemma that applies much more generally to groups:

Lemma: Let $h : X \rightarrow Y$ be a group homomorphism, with finite groups X, Y . Let Z, W be subgroups of Y , with $Z \supset W$, and suppose that Z is contained in the image $f(X)$ of f . Put

$$h^{-1}(Z) = \{g \in G : h(g) \in Z\}$$

$$h^{-1}(W) = \{g \in G : h(g) \in W\}$$

Then we have a formula regarding *indices*:

$$[Z : W] = [h^{-1}(Z) : h^{-1}(W)]$$

Proof: Let V be the kernel of the homomorphism $h : X \rightarrow Y$. We will prove that

$$|h^{-1}(Z)| = |V| \cdot |Z|$$

and, similarly,

$$|h^{-1}(W)| = |V| \cdot |W|$$

As soon as we know that these equalities hold, then

$$[Z : W] = \frac{|Z|}{|W|} = \frac{|V| \cdot |Z|}{|V| \cdot |W|} = \frac{|h^{-1}(Z)|}{|h^{-1}(W)|} = [h^{-1}(Z) : h^{-1}(W)]$$

The *inverse image* $h^{-1}(Z)$ of Z is the disjoint union of the *inverse images*

$$h^{-1}(z) = \{x \in X : h(x) = z\}$$

of elements $z \in Z$. If we can prove that

$$\text{number of elements in } h^{-1}(z) = |V|$$

then it will follow that

$$\begin{aligned} |h^{-1}(Z)| &= \text{sum of cardinalities of sets } h^{-1}(z) \text{ for } z \text{ in } Z \\ &= |Z| \cdot |V| \end{aligned}$$

since there are $|Z|$ different sets $h^{-1}(z)$ and we anticipate that each one has cardinality $|V|$.

Thus, the problem is reduced to showing that

$$\text{number of elements in } h^{-1}(z) = |V|$$

for any $z \in Z$. To do this, let's make a bijection

$$b : V \rightarrow h^{-1}(z)$$

This would prove that the sets have the same number of elements, without directly counting. Since z is in the image of h , we can find at least one $x_o \in X$ so that $h(x_o) = z$. With this in hand, let's try

$$b(v) = v \cdot x_o$$

First we have to check that this really maps from V to $h^{-1}(z)$. That is, we must check that

$$h(b(v)) = z \text{ for all } v \in V$$

Indeed,

$$h(b(v)) = h(v \cdot x_o) = h(v) \cdot h(x_o) = e_Y \cdot z = z$$

since v is in the kernel V of h . Next, let's check that b is *injective*: suppose that $b(v) = b(v')$ for $v, v' \in V$. That is, we assume that

$$v \cdot x_o = v' \cdot x_o$$

By right multiplying by x_o^{-1} and simplifying, we get $v = v'$, so b is indeed injective. Last, check surjectivity: given $q \in h^{-1}(z)$, find $v \in V$ so that $q = b(v)$. Let's check that $q \cdot x_o^{-1} \in V$ hits q :

$$h(q \cdot x_o^{-1}) = h(q) \cdot h(x_o^{-1}) = z \cdot h(x_o)^{-1} = z \cdot z^{-1} = e_Z$$

This finishes the proof that $b : V \rightarrow h^{-1}(z)$ is a bijection, proving that the number of elements in $h^{-1}(z)$ is equal to $|V|$. Thus, this finishes the proof of the Lemma. ♣

Corollary: We have

$$[I : K] = [f^{-1}(S) : f^{-1}(\{e\})] = [S : \{e\}] = 2^N$$

Proof: From the definition of f as $f(g) = g^\ell$,

$$K = f^{-1}(\{e\})$$

And another lemma above proved that

$$I = f^{-1}(S)$$

By the previous lemma,

$$[f^{-1}(S) : f^{-1}(\{e\})] = [S : \{e\}]$$

which is the same thing as $|S|$. Since S consists of choices of ± 1 for each of the N different primes p_i dividing n , $|S| = 2^N$. This proves the corollary. ♣

Using the last lemma again, we also have:

Corollary: Let $P = \{\pm 1 \pmod n\}$, and $E = \{e_G\}$. We have

$$[J : K] = [f^{-1}(P) : f^{-1}(E)] = [P : E] = 2$$

Now we are in the situation that $I \supset J \supset K$ and $[I : K] = 2^N$ and $[J : K] = 2$. In the original discussion of group indices, we proved the multiplicative property

$$[I : J] \cdot [J : K] = [I : K]$$

Thus,

$$[I : J] = [I : K] / [J : K] = 2^{N-1}$$

Since also $[G : J] = [G : I] \cdot [I : J]$, surely

$$[G : J] \geq [I : J] = 2^{N-1}$$

Since the strong (Miller-Rabin) liars are all contained in J , we see that

$$\frac{\text{number of liars}}{|G|} \leq \frac{1}{2^{N-1}}$$

If the number N of distinct prime factors of n is at least 3, then we have

$$\frac{\text{number of liars}}{|G|} \leq \frac{1}{4}$$

If the number N of distinct prime factors is 2, then we know by now that n cannot be a Carmichael number. That is, the group denoted H above is a *proper* subgroup of $G = \mathbf{Z}/n^\times$. That is, by Lagrange's theorem, $[G : H] \geq 2$. Then from the multiplicative property of subgroup indices (applied repeatedly) we have in this case

$$[G : J] = [G : H] \cdot [H : I] \cdot [I : J] \geq [G : H] \cdot [I : J] \geq 2 \cdot 2^1 = 4$$

Thus, also in this case, we conclude that the liars make up less than 1/4 of all the elements of G .

Finally, suppose that $n = p^e$, a power of a single prime p . (This is the case $N = 1$.) In this case we know from the existence of primitive roots that $\mathbf{Z}/p^{e \times}$ is *cyclic*. The group H in this case becomes

$$H = \{g \in \mathbf{Z}/p^{e \times} : g^{p^e - 1} = 1 \pmod{p^e}\}$$

From our discussion of cyclic groups, to determine $|J|$ we can use the *isomorphism* of the multiplicative group $\mathbf{Z}/p^{e \times}$ with the additive group $\mathbf{Z}/\varphi(p^e)$. Converting to additive notation, we want to know the number of solutions x to the equation

$$(p^e - 1) \cdot x = 0 \pmod{\varphi(p^e)}$$

This is

$$(p^e - 1) \cdot x = 0 \pmod{(p - 1)p^{e-1}}$$

We have solved such congruences before: taking out the common factor, this is equivalent to

$$\frac{p^e - 1}{p - 1} \cdot x = 0 \pmod{p^{e-1}}$$

Now the coefficient of x is relatively prime to the modulus, so has a multiplicative inverse, and this is equivalent to

$$x = 0 \pmod{p^{e-1}}$$

Since x is an integer modulo p^e , we see that we get exactly $p - 1$ different solutions mod $\varphi(p^e)$.

Thus,

$$[G : J] = [G : H] \cdot [H : J] \geq [G : H] = \frac{\varphi(p^e)}{p - 1} = p^{e-1}$$

Except for the case $p = 3$ and $e = 2$ we obtain the necessary $[G : J] \geq 4$. From this we conclude again in this case that at most $1/4$ of the possible candidates are liars.

The remaining special case of $n = 9$ can be treated directly: there are just two strong liars, ± 1 , and $2/(9 - 1) = 1/4$.

At long last, this finishes the proof of the theorem, demonstrating that the Miller-Rabin test works. ♣

24. More on groups

- Cauchy's Theorem
 - Normal subgroups, quotient groups
 - Isomorphism Theorems
 - Automorphisms of groups
 - Sylow's theorem
 - Product groups and direct sum groups
 - Finite abelian groups
-

24.1 Cauchy's Theorem

When we go from the most special groups, *cyclic* ones, to the general case where we assume nothing but that the groups in question are *finite*, our expectations must be more modest.

The results here would seem disappointingly weak if we were unacquainted with the otherwise grueling task of *trying to find all the subgroups of a given group*. In that context, Lagrange's Theorem gives a very strong limitation on the possible orders of subgroups. The new result, **Cauchy's Theorem**, gives a little bit in the other direction.

- (*Lagrange*): Let G be a *finite* group. Then the order of any subgroup H of G divides the order of G . The order of any *element* divides the order of the group.
- (*Cauchy*): Let G be a *finite* group, and let p be a *prime* dividing the order of G . Then there is a subgroup of G of order p .
- *Caution*: It is not generally true that for every divisor of the order of a finite group there is a subgroup of that order. And even if there is one, there may be more than one, so uniqueness fails in general, too.

There are some crucial corollaries of Lagrange's theorem to remember:

- A group of prime order is *cyclic*.
 - A group of order p^2 for some prime p is *abelian*.
-

24.2 Normal subgroups, quotient groups

In this section we pick out a very important property that a subgroup may or may not have, and then look at another construction of new groups from old.

First, there is an important bit of notation: for a subgroup H of a group G , and for $g \in G$, we write

$$gHg^{-1} = \{ghg^{-1} : h \in H\}$$

A subgroup N of a group G is **normal** or **invariant** if it has the property that

$$gNg^{-1} \subset N$$

for every $g \in G$.

- The kernel N of a group homomorphism $f : G \rightarrow H$ is a normal subgroup of G .

Proof: Let $g \in G$ and take $n \in N$. Then

$$f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g)ef(g)^{-1} = e$$

using the definition of what a homomorphism is, since we know that $f(g^{-1}) = f(g)^{-1}$. Thus, gng^{-1} is also in the kernel. That is, we have shown that $gNg^{-1} \subset N$, as required by the definition of ‘normality’. *Done.*

Now we can define a **quotient group**, written G/N , for a normal subgroup N of G . First, the *set* of element of G/N is the *set of cosets* gN of N . The group law is

$$g_1H \star g_2H = (g_1g_2)H$$

The **identity** $e_{G/N}$ in the quotient is the ‘trivial coset’ $H = eH$ of H . And the **inverse** of gH is $g^{-1}H$. (Of course, the assertions that these things are as claimed need proof!)

This new entity, the “quotient group” G/N can also be described as a collection of *equivalence classes*, as follows. For a subgroup N of a group G , define a relation \sim by

$$x \sim y \quad \text{if and only if} \quad xN = yN$$

Before proving that th definition really makes G/N a *group*, one might ask: *Why do we need N to be normal?* The answer lies inside the proof that we really have a group: if N is *not* normal then we are unable to define a reasonable group operation on G/N !

Proof that G/N is a group: We grant ourselves the little exercise that if N is normal then for any $g \in G$ we have

$$gN = Ng$$

Let’s check first that $N = eN$ is the identity in G :

$$(eN) \star (gN) = (eg)N = gN$$

(And we’d already seen that we only need to check multiplication on one side only in order to verify that an element is the identity).

Next,

$$(gN)(g^{-1}N) = (gg^{-1})N = eN = N$$

so $g^{-1}N$ is indeed the inverse of gN . So there are inverses.

Associativity follows from the associativity in the group G .

A subtler issue, and one upon which the sensibility of this whole discussion depends, is **well-definedness**: this is an issue that does not come up in more elementary situations, or at least can be easily hidden there. The issue is perhaps a surprising one: if $sH = tH$, does it follow that

$$(gN) * (sN) = (gN) * (tN) ?$$

It surely would be awful if this didn't work! Well, the thing is to *relate this 'made-up' group operation to tangible operations, and use the normality*:

$$\begin{aligned}(gN) * (hN) &= (gh)N = (gh)NN = g(hN)N = g(Nh)N \quad (\text{using normality!}) \\ &= (gN)(hN)\end{aligned}$$

That is, the group operation is really the 'subset multiplication' inside G , if we can safely assume that the subgroup is normal. This gives the well-definedness, since the multiplication

$$(gN) * (hN) = (gN)(hN)$$

is now really defined in terms of the *cosets* gN and hN , and *not just* in terms of the elements g, h used to *name them*. Thus, with $sN = tN$,

$$\begin{aligned}(gN) * (sN) &= (gN)(sN) \quad (\text{by previous discussion}) \\ &= (gN)(tN) \quad (\text{since we suppose that } sN = tN) \\ &= (gN) * (tN) \quad (\text{by previous discussion})\end{aligned}$$

This is what well-definedness involves. We are *done* with the proof.

So the normality of the subgroup is essential to know that the 'group operation' on the quotient really is any kind of operation at all (that is, is well-defined)!

The simplest and one of the most important examples of a quotient group is \mathbf{Z}/n . In this case the group is $G = \mathbf{Z}$, of course, and the normal subgroup is

$$N = n\mathbf{Z} = \{nx : x \in \mathbf{Z}\} = \text{multiples of } n$$

Recall that all along we have talked in a funny way about the 'entities' in \mathbf{Z}/n being integers-mod- n rather than simply integers. This was to avoid confrontation about integers-mod- n 'really' being cosets, although that's exactly what we were doing all along. Indeed, *using additive notation*, really

$$x\text{-mod-}n = x + n\mathbf{Z}$$

The fact that $N = n\mathbf{Z}$ is *normal* is a very special case of the fact that any subgroup of an abelian group is normal.

At the very outset of the discussion of $\mathbf{Z}\text{-mod-}n$, there was the issue of checking that if

$$x\text{-mod-}n = x'\text{-mod-}n \quad \text{and} \quad y\text{-mod-}n = y'\text{-mod-}n$$

then

$$(xy)\text{-mod-}n = (x'y')\text{-mod-}n \quad \text{and} \quad (x+y)\text{-mod-}n = (x'+y')\text{-mod-}n$$

This is the same issue of *well-definedness* that arose in verification that the operation in a quotient group really works right.

To prove well-definedness usually amounts to showing that the definition of something does not depend excessively on the notation, but really only on the underlying *thing*.

24.3 Isomorphism Theorems

The spirit of the result here is that some things which seemed different are really the same. This is good.

Theorem: (*Isomorphism Theorem(s)*)

- Let $f : G \rightarrow H$ be a *surjective* group homomorphism. Let N be the *kernel* of f . Then the map

$$\bar{f} : G/N \rightarrow H$$

defined by

$$\bar{f}(gN) = f(g)$$

is *well-defined* and gives an *isomorphism* from G/N to H .

- Let N, H be subgroups of a group G , with N normal. Suppose that $N \cdot H = G$. Then we have an *isomorphism*

$$f : H/(H \cap N) \rightarrow G/N$$

given by

$$f(h(H \cap N)) = hN$$

Proof: First we have to prove the well-definedness of \bar{f} . That is, we must show that if $gN = g'N$ then $\bar{f}(g) = \bar{f}(g')$ (for $g, g' \in G$). Again, the point is that the *notation* “ gN ” for a coset should not matter, but only the actual coset itself. If $gN = g'N$, then (by left multiplying by g^{-1}) we get $N = g^{-1}g'N$. In particular, this says that $N \ni g^{-1}g'$. Thus, $f(g^{-1}g') = e_H$. Using the group homomorphism property, this gives $f(g^{-1})f(g') = e_H$. By now we know that homomorphisms preserve inverses, so $f(g)^{-1}f(g') = e_H$, from which we obtain $f(g') = f(g)$ by left multiplication by $f(g)$. This proves the well-definedness of \bar{f} .

Next we prove that \bar{f} is a group homomorphism. For $g, g' \in G$ we have

$$\bar{f}(gN \cdot g'N) = \bar{f}(gg' \cdot N) = f(gg') = f(g) \cdot f(g') = \bar{f}(gN) \cdot \bar{f}(g'N)$$

which is the desired property.

Next prove *surjectivity* of \bar{f} . Let $h \in H$. Since f is surjective, there is $g \in G$ so that $f(g) = h$. Then $\bar{f}(gN) = f(g) = h$, so \bar{f} is also surjective.

Next, *injectivity*: Suppose that $\bar{f}(gN) = \bar{f}(g'N)$. Then by the definition of f this gives $f(g) = f(g')$. That is, left multiplying by $f(g)^{-1}$, $e_H = f(g)^{-1} \cdot f(g')$. Since group homomorphisms respect inverses, this gives $e_H = f(g^{-1}g')$. Therefore, $g^{-1}g' \in N$, since N is the kernel of f . Then $gN = g'N$ (reversing an argument given just above!) This is the desired injectivity. And this proves the first assertion of the Theorem.

Now consider the second part of the theorem. We must prove well-definedness, the homomorphism property, and injectivity and surjectivity.

First we prove well-definedness. That is, suppose that $h, h' \in H$, and that $h(H \cap N) = h'(H \cap N)$, and prove that $hN = h'N$. In particular, we have $h' \in h(H \cap N)$. That is, there is $m \in H \cap N$ so that $h' = hm$. Then

$$h'N = (hm)N = h(mN) = hN$$

This proves well-definedness.

To see the homomorphism property:

$$f(h(H \cap N) \cdot h'(H \cap N)) = f(hh' \cdot (H \cap N)) = hh' \cdot N$$

$$= (hN) \cdot (h'N) = f(h(H \cap N)) \cdot f(h'(H \cap N))$$

which is the desired property.

For surjectivity, we use the hypothesis that for every $g \in G$ there is $h \in H$ and $n \in N$ so that $g = hn$. Then $gN = (hn)N = hN$. That is, $f(h(H \cap N)) = gN$. This is surjectivity.

For injectivity, suppose $hN = h'N$. Then $h' \in hN$, and (left multiplying by h^{-1} we have $h^{-1}h' \in N$. But also since H is a *group* it must be that $h^{-1}h' \in H$. Therefore, $h^{-1}h' \in (H \cap N)$. Thus, going back in the other direction,

$$h' \cdot (H \cap N) = h \cdot (H \cap N)$$

as desired. This finishes the proof of the theorem. *Done.*

24.4 Automorphisms of groups

This section has some importance in its own right, and also can be viewed as an example of *how groups occur naturally*.

An **automorphism** of a group G is a *group isomorphism*

$$f : G \rightarrow G$$

of G to itself. The **identity automorphism** or **trivial automorphism** is the isomorphism $i : G \rightarrow G$ so that $i(g) = g$ for all $g \in G$. Any group has this kind of automorphism.

And if f is an automorphism of G , then the *inverse function* f^{-1} can also be checked to be an isomorphism. And the *composite* of two isomorphisms can be checked to be an isomorphism. Therefore, *the set of all automorphisms of a group G is itself a group, denoted*

$$\text{Aut}(G) = \{ \text{all automorphisms of } G \}$$

In general, it is very hard to figure out what the automorphism group of a given group is. However, in one happy case the answer is very easy and clear:

All automorphisms of \mathbf{Z}/N are of the form

$$f_y(x) = y \cdot x$$

where $y \in \mathbf{Z}/N^\times$. Thus, with this notation, the map

$$y \rightarrow f_y$$

gives an isomorphism of \mathbf{Z}/N^\times to the automorphism group $\text{Aut}(\mathbf{Z}/N)$ of \mathbf{Z}/N .

Since any finite cyclic group is isomorphic to \mathbf{Z}/N for some N , this result tells the automorphism group of any finite cyclic group.

There are just two automorphisms of \mathbf{Z} : the trivial automorphism and the automorphism $x \rightarrow -x$. This also describes the automorphism group of *infinite cyclic* groups, since every infinite cyclic group is isomorphic to \mathbf{Z} .

24.5 Sylow's theorem

Beyond Lagrange's theorem and Cauchy's theorem, the most basic result for beginning to try to see 'what groups there are' is Sylow's Theorem. If we take the view that Cauchy's theorem is an assertion of *existence of subgroups*, then we should view Sylow's theorem as a great improvement upon Cauchy's. In particular, it is strong enough so that we can *classify up to isomorphism* all groups of certain small sizes, simply by using *divisibility arguments*, as we'll see after the statement of the theorem.

Let G be a finite group of order N . Fix a prime number p and let p^n be the largest power of p dividing the order of G . A **Sylow p -subgroup** of G is a subgroup of order p^n (if there is one). By Lagrange's theorem, these are the largest p -power-order subgroups possible in G .

- For every prime p dividing $|G|$, a finite group G has Sylow p -subgroups.
- The number of Sylow p -subgroups is congruent to 1 modulo p .

Example: Let's show that *any group of order 15 is cyclic*. If there is an element g of order 15, then necessarily $\langle g \rangle$, and we're done. Suppose then that there is *no* element of order 15 (and hope to get a contradiction). Then we *count* the number of elements in the whole group in two different ways. First, of course, the total number is 15. On the other hand, we can count how many elements there are of each possible order. By Lagrange's theorem, the only possible orders of elements are 1, 3, 5, 15. There is just one element of order 1, the identity. By assumption, there is no element of order 15. There are $3 - 1$ elements of order 3 in a subgroup of order 3, and similarly $5 - 1$ elements of order 5 in a subgroup of order 5.

By Sylow's theorem we know that there are non-negative integers x, y so that

$$3x + 1 = \text{number of subgroups of order 3}$$

$$5y + 1 = \text{number of subgroups of order 5}$$

But we must pay attention to possible overlap of these subgroups in order to have a correct counting. If P, Q are two different subgroups, of orders either 3 or 5, then the order of the *intersection* is a *proper* divisor of both numbers (by Lagrange), so must be just 1. That means that

$$\begin{aligned} \text{number of elements of order 3} &= (3 - 1) \cdot \text{number of subgroups of order 3} \\ &= 2 \cdot (3x + 1) \end{aligned}$$

$$\begin{aligned} \text{number of elements of order 5} &= (5 - 1) \cdot \text{number of subgroups of order 5} \\ &= 4 \cdot (5y + 1) \end{aligned}$$

Comparing the two counts (under the hypothesis, remember, that there are no elements of order 15) gives

$$15 = 1 + 2(3x + 1) + 4(5y + 1)$$

Simplifying, this is

$$4 = 3x + 10y$$

with x, y non-negative integers. But this is impossible. Thus, it is impossible that there be no element of order 15, so it is impossible that a group of order 15 *not* be cyclic.

There are further parts to Sylow's theorem. One part which is useful for dealing with groups which have orders which are powers of p is

- The *center* of a Sylow p -subgroup is *non-trivial*, that is, is strictly larger than the trivial subgroup $\{e\}$.

Example/Corollary: Let p be a prime. Using this last part of the Sylow theorem, one can prove

- Every group G of order p^2 is abelian.

There is yet more to Sylow's theorem: Let H be a subgroup of G . Use notation that for any fixed $g \in G$

$$gHg^{-1} = \{ghg^{-1} : h \in H\}$$

The element ghg^{-1} is **the conjugate of h by g** . Two subgroups H, K of G are **conjugate** (to each other) if there is some $g \in G$ so that

$$gHg^{-1} = K$$

We would say that K is **the conjugate of H by g** .

- Any two Sylow p -subgroups are *conjugate* in G .
 - Every subgroup H of G with $|H|$ a power of p lies inside some Sylow p -subgroup.
-

24.6 Product groups and direct sum groups

We are acquainted with some simple sorts of groups, such as \mathbf{Z}/N (with addition modulo N), and now we describe a process to assemble such 'atoms' into larger groups.

Let G, H be two groups. The **product group**

$$G \times H$$

is defined to be the set of *ordered pairs* (g, h) (with $g \in G, h \in H$) with **component-wise group operation**:

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$$

Thus, this product group is just the Cartesian product (set) of the two sets, with the component-wise group operation.

This can be generalized a little. Let G_1, \dots, G_n be groups. The **product group**

$$G_1 \times \dots \times G_n$$

is defined to be the set of *ordered n -tuples* (g_1, \dots, g_n) (with $g_i \in G_i$) with **component-wise group operation**:

$$(g_1, \dots, g_n)(g'_1, \dots, g'_n) = (g_1g'_1, \dots, g_ng'_n)$$

Yes, this does resemble notation for vectors. In fact, the direct sum

$$\mathbf{R} \oplus \dots \oplus \mathbf{R} \quad (n \text{ copies})$$

is exactly the usual Euclidean n -space, except that we've overlooked scalar multiplication.

Similarly,

$$\mathbf{Z} \oplus \dots \oplus \mathbf{Z} \quad (n \text{ copies})$$

can reasonably be viewed as the collection of n -dimensional *integer* vectors.

Sometimes, especially when the groups involved in a product are *abelian*, a product of groups is written in a different way, and is called a **direct sum**: for abelian groups G_1, \dots, G_n we would write

$$G_1 \times \dots \times G_n = G_1 \oplus \dots \oplus G_n$$

Not only can we make bigger groups from smaller by this procedure, in some cases we can go in the other direction and express a big group as a product, thereby ‘explaining’ its structure. The fundamental example of this is in the next section.

24.7 Finite abelian groups

Having seen a little example of how Sylow’s theorem (which applies to all *finite* groups) can be used to examine the possibilities for groups of a given order, let’s add an important hypothesis, that of *abelian-ness*.

As it happens, the class of *finite abelian groups* can be described completely in terms of elementary divisibility and the groups \mathbf{Z}/N , as follows.

- Given a finite abelian group G , there is a uniquely-determined integer $m > 0$ and uniquely-determined sequence of numbers d_1, d_2, \dots, d_m with the *divisibility property*

$$d_1 | d_2 | d_3 | \dots | d_m$$

and so that

$$G \approx \mathbf{Z}/d_1 \oplus \mathbf{Z}/d_2 \oplus \mathbf{Z}/d_3 \oplus \dots \oplus \mathbf{Z}/d_m$$

The positive integers d_1, d_2, \dots, d_m occurring in such an expression for a finite abelian group are the **elementary divisors** of the group.

Thus, every finite abelian group can be ‘decomposed’ or ‘broken up’ into simpler pieces, each of which is one of the relatively elementary groups \mathbf{Z}/N .

This reduces classification of all finite abelian groups of a given order to yet another question in elementary arithmetic.

For example, let’s find all the abelian groups of order 12. We must find a sequence of integers, each dividing the next, whose product is 12. In this simple example we can ‘see’ the possibilities for the elementary divisors: the only possibilities are

$$\mathbf{Z}/2 \oplus \mathbf{Z}/6$$

and

$$\mathbf{Z}/12$$

Let’s find all abelian groups of order 48. This is still easy to do without a systematic approach:

$$\mathbf{Z}/48$$

$$\mathbf{Z}/2 \oplus \mathbf{Z}/24$$

$$\mathbf{Z}/4 \oplus \mathbf{Z}/12$$

$$\mathbf{Z}/2 \oplus \mathbf{Z}/2 \oplus \mathbf{Z}/12$$

$$\mathbf{Z}/2 \oplus \mathbf{Z}/2 \oplus \mathbf{Z}/2 \oplus \mathbf{Z}/6$$

#24.182 Let p be a prime. Suppose that a group G has p elements. Prove that G is *cyclic*.

#24.183 Suppose that a finite group G has no subgroups but $\{e\}$ and G . Show G is cyclic.

#24.184 Let G be a group of order n . Show that for all $g \in G$ we have $g^n = e$.

#24.185 Let m, n be relatively prime. Let H, K be subgroups of a group G where $|H| = m$ and $|K| = n$. Show that $H \cap K = \{e\}$.

#24.186 Fix a prime p . Suppose all *proper* subgroups of a finite group G have orders powers of p . Prove that $|G|$ is a power of p .

#24.187 Let p, q be distinct primes. Show that any *abelian* group of order pq has an element of order pq , so is *cyclic*.

#24.188 Let N be a normal subgroup of group G , and show that not only is it that $gNg^{-1} \subset N$, but in fact $gNg^{-1} = N$.

#24.189 Show that a subgroup N of a group G is normal if and only if $gN = Ng$ for all $g \in G$.

#24.190 Show that in an *abelian* group *every* subgroup is normal.

#24.191 Show that for *any* subgroup H of a group G (with H not necessarily *normal* in G), the relation defined by

$$x \sim y \quad \text{if and only if} \quad xH = yH$$

is an equivalence relation.

#24.192 Show that a homomorphism $f : G \rightarrow H$ is *injective* if and only if its kernel is *trivial*, that is, if and only if its kernel is the *trivial subgroup* $\{e\}$ of G . (*Hint:* On one hand, if $f(g) = f(g')$ then $e_H = f(g)^{-1}f(g') = f(g^{-1}g')$ so $g^{-1}g'$ is in the kernel. If $g \neq g'$ then this gives a non-trivial (not equal to e_G) element of the kernel. On the other hand, reversing this argument you can show that if the kernel is trivial (is just $\{e_G\}$) then $f(g) = f(g')$ implies that $g = g'$).

#24.193 Let $f : G \rightarrow H$ and $g : G \rightarrow K$ be two group homomorphisms. Let

$$F : G \rightarrow H \oplus K$$

be defined by

$$F(x) = (f(x), g(x))$$

Show that

$$\ker F = \ker f \cap \ker g$$

#24.194 Let m, n be relatively prime positive integers. Let

$$f : \mathbf{Z}/mn \rightarrow \mathbf{Z}/m$$

be defined by

$$f(x - \text{mod} - mn) = x \text{ mod } m$$

and also define

$$g : \mathbf{Z}/mn \rightarrow \mathbf{Z}/n$$

by

$$g(x - \text{mod} - mn) = x \text{ mod } n$$

Then also define

$$F : \mathbf{Z}/mn \rightarrow \mathbf{Z}/m \oplus \mathbf{Z}/n$$

by

$$f(x - \text{mod} - mn) = (f(x), g(x))$$

First show that the intersection of the kernels of f and of g is *trivial*. From this conclude that the kernel of F is trivial, so that F is *injective*. Then, by counting, deduce that F is also *surjective*, so is an isomorphism).

#24.195 Let N be a normal subgroup of a group G . Let $f : G \rightarrow H$ be a group homomorphism whose kernel contains N . Show that the map

$$\bar{f} : G/N \rightarrow H$$

defined by

$$\bar{f}(gN) = f(g)$$

is *well-defined* and is a group homomorphism. (*Hint*: To prove well-definedness usually amounts to showing that the definition of something does not depend excessively on the notation, but really only on the underlying *thing*).

#24.196 Let G be a cyclic group of (finite) order N , with generator g . Show that G is isomorphic to \mathbf{Z}/N , by showing that the map $f : G \rightarrow \mathbf{Z}/N$ defined by $f(g^n) = n \text{-mod-} N$ is such an isomorphism.

#24.197 Let G be a cyclic group of infinite order, with generator g . Show that G is isomorphic to \mathbf{Z} , by showing that the map $f : G \rightarrow \mathbf{Z}$ defined by $f(g^n) = n$ is such an isomorphism.

#24.198 Let $f_1 : G \rightarrow H_1$ and $f_2 : G \rightarrow H_2$ be group homomorphisms. Define

$$f : G \rightarrow H_1 \oplus H_2$$

by

$$f(g) = (f_1(g), f_2(g))$$

Show that this f is a group homomorphism.

#24.199 Let m, n be *relatively prime* positive integers. Define

$$f : \mathbf{Z}/mn \rightarrow \mathbf{Z}/m \oplus \mathbf{Z}/n$$

by (using additive notation)

$$f(x + mn\mathbf{Z}) = (x + m\mathbf{Z}, x + n\mathbf{Z})$$

Show that this is an *isomorphism*. (*Hint*: In effect, this says that a system of congruences

$$x \equiv a \pmod{m} \quad x \equiv b \pmod{n}$$

can always be solved for x for any a, b , and that the solution x is uniquely determined modulo mn . Use the fact that there are integers s, t so that $sm + tn = 1$. Try $x = bsm + atn$?)

#24.200 Find an integer x so that $x \equiv 2 \pmod{10}$ and $x \equiv 7 \pmod{11}$. Then find a *different* integer x' with the same property.

#24.201 Fix an element g_o of a group G . Show that both maps L, R defined by

$$L(g) = g_o g \quad R(g) = g g_o$$

are *bijections* of G to itself.

#24.202 Let x, y be fixed elements in a group G . Fix a subset S of G , and let $T = xSy$. Show that the map

$$f(g) = xgy$$

(which is defined on all of G) does indeed map S to T , and gives a *bijection* from S to T . (Compare to the previous exercise!)

#24.203 Fix a subgroup H of a group G and fix $g \in G$. Show that the *conjugate* gHg^{-1} of H by g is a subgroup. (And observe that the previous exercise shows that gHg^{-1} has the same order as does H).

#24.204 Show that a group homomorphism $f : G \rightarrow H$ is *injective* if and only if its kernel is ‘trivial’, meaning that $\ker f = \{e\}$.

#24.205 Let G be a group. For $h \in G$ define $f_h : G \rightarrow G$ by $f_h(g) = hgh^{-1}$. Prove that f_h is an automorphism of G . (Such automorphisms are called **inner automorphisms**).

#24.206 Let G be an *abelian* group. Prove that $f(g) = g^{-1}$ is an automorphism of G .

#24.207 Let g be a generator for a cyclic group G . Let $f : G \rightarrow G$ be an *automorphism* of G . Show that $f(g)$ is also a generator of G . (*Hint*: Automorphisms are bijections, so every element in G can be written as $f(h)$ for some $h \in G$. So to prove $\langle f(g) \rangle = G$ it suffices to prove that for each $h \in G$ there is $\ell \in \mathbf{Z}$ so that $f(g)^\ell = f(h)$.)

#24.208 Grant that *automorphisms send generators to generators*. Prove that all automorphisms of \mathbf{Z}/N are of the form

$$f(x \bmod N) = rx \bmod N$$

for some $r \in \mathbf{Z}/N^\times$. (*Hint*: we know all possible generators of \mathbf{Z}/N).

#24.209 Grant that *automorphisms send generators to generators*. Prove that there are exactly 2 automorphisms of \mathbf{Z} : the identity map and the map $f(x) = -x$.

#24.210 Show that every group of order 33 is cyclic. (*Hint*: Use Sylow’s theorem).

#24.211 Show that every group of order 85 is cyclic. (*Hint*: Use Sylow’s theorem).

#24.212 Using the Sylow Theorem, show that in a group of order pq with two primes p, q and $p < q$, there is only *one* subgroup of order q (by a counting argument).

#24.213 Granting that in a group of order pq with two primes p, q and $p < q$, there is only *one* subgroup of order q , show that this subgroup is necessarily *normal*.

#24.214 Show that the order of a product group $G \times H$ is the product $|G| \times |H|$ of the orders $|G|, |H|$ of the two groups.

#24.215 Find all *abelian* groups of order 12.

#24.216 Find all *abelian* groups of order 125.

#24.217 Find all *abelian* groups of order 127.

#24.218 Find all *abelian* groups of order 64.

#24.219 Find all *abelian* groups of order $2^2 \cdot 3^2 \cdot 5^2$.

#24.220 Find all *abelian* groups of order $2^2 \cdot 3^2 \cdot 5^3$.

25. Finite fields

While we are certainly accustomed to (and entitled to) think of the *fields* rationals, reals, and complex numbers as ‘natural’ batches of numbers, it is important to realize that there are *many* other important *fields*. Perhaps unexpectedly, there are many *finite* fields:

For example

- For a prime number p , the quotient \mathbf{Z}/p is a *field* (with p elements).

After seeing what the proof of the latter fact entails, this ought not seem so surprising: We can already grant ourselves that \mathbf{Z}/p is a *commutative ring with unit*, being the quotient of \mathbf{Z} by the ideal $p\mathbf{Z}$. So the issue is only to check that *every non-zero element has a multiplicative inverse*. Let $x \in \mathbf{Z}/p$ be non-zero: that means that $x = y + p\mathbf{Z}$ for some integer y not divisible by p . Then, for example computing via the Euclidean algorithm, there are integers s, t so that $sy + tp = \gcd(y, p) = 1$. Then $sy \equiv 1 \pmod{p}$. Therefore, $s + p\mathbf{Z}$ will be a multiplicative inverse of $y + p\mathbf{Z} = x$. That is, any non-zero element has a multiplicative inverse, so \mathbf{Z}/p is a *field*.

In particular, we see that for each prime number p there is indeed a (finite!) field with p elements.

On the other hand, for example, *there is no finite field with 6 or with 10 elements*.

While it turns out that there *are* finite fields with, for example, 9 elements, 128 elements, or *any prime power* number of elements, it requires a bit more preparation to ‘find’ them.

The simplest finite fields are the rings \mathbf{Z}/p with p prime. For many different reasons, we want *more* finite fields than just these. One immediate reason is that for machine implementation (and for other computational simplifications) it is optimal to use fields *of characteristic 2*, that is, in which $1 + 1 = 2 = 0$. Among the fields \mathbf{Z}/p only $\mathbf{Z}/2$ satisfies this condition. At the same time, for various reasons we might want the field to be *large*. If we restrict our attention to the fields \mathbf{Z}/p we can’t meet both these conditions simultaneously.

This section sets up a viewpoint adequate to these tasks, along with necessary technical preparation.

- Ideals in commutative rings
- Ring homomorphisms
- Quotient rings
- Maximal ideals and fields
- Field extensions
- Sums and products in field extensions
- Multiplicative inverses in field extensions

25.1 Ideals in commutative rings

The concept of **ideal** in a commutative ring is a sort of generalization of the concept of *number*. In fact, originally there was a closely related notion of *ideal number* which extended the usual notion of number. This phrase has since been shortened simply to “ideal”.

Let R be a commutative ring with unit 1. An **ideal** in R is a subset I of R so that

- For all $r \in R$ and $x \in I$ we have $r \cdot x \in I$. (Closure under multiplication by ring elements.)
- For all $x, y \in I$ we have $x + y \in I$. (Closure under addition.)
- For all $x \in I$ we have $-x \in I$. (Closure under inverse.)
- $0 \in I$.

The second, third, and fourth conditions can be capsulized as requiring that I -with-addition must be a subgroup of the additive group R -with-addition.

The first condition may seem a little peculiar. For one thing, it is a stronger requirement than that I be a *subring* of R , since we require that I be closed under multiplication by elements of R , not merely by elements of I itself.

Example: The basic example is the following. In the ring \mathbf{Z} , for any fixed n , the set $n \cdot \mathbf{Z}$ consisting of all multiples of n is an ideal. Indeed, if $x = mn$ is a multiple of n , and if $r \in \mathbf{Z}$, then $r \cdot x = r(mn) = (rm)n$ is still a multiple of n . Likewise, 0 is contained in $n\mathbf{Z}$, it's closed under sums, and closed under additive inverses.

Example: Let $R = k[x]$ be the ring of polynomials in one variable x with coefficients in a field k . Fix a polynomial $P(x)$, and let $I \subset R$ be the set of all polynomial multiples $M(x) \cdot P(x)$ of $P(x)$. Verification that I is an ideal is identical in form to the previous example.

Example: Abstracting the previous two examples: let R be any commutative ring with unit 1, and fix $n \in R$. Then the set $I = n \cdot R = \{mn : m \in R\}$ is an ideal, called the **principal ideal generated by n** . The same argument proves that it is an ideal. Such an ideal is called a **principal ideal**.

Example: In any ring, the **trivial ideal** is just the set $I = \{0\}$. Consistent with typical usage in mathematics, an ideal I is **proper** if it is neither the trivial ideal $\{0\}$ nor the whole ring R (which is also an ideal).

The following proposition is an important basic principle.

Proposition: Let I be an ideal in a commutative ring R with unit 1. If I contains any element $u \in R^\times$, then $I = R$.

Proof: Suppose I contains $u \in R^\times$. The fact that u is a unit means that there is a multiplicative inverse u^{-1} to u . Then, for any $r \in R$,

$$r = r \cdot 1 = r \cdot (u^{-1} \cdot u) = (r \cdot u^{-1}) \cdot u$$

That is, r is a multiple of u . Since I is an ideal, it must contain every multiple of u , so I contains r . Since this is true of every element $r \in R$, it must be that $R = I$. ♣

Corollary: Let I be an ideal in a polynomial ring $k[x]$ where k is a field. If I contains any non-zero ‘constant’ polynomial, then $I = k[x]$.

Proof: This will follow from the previous proposition if we check that non-zero constant polynomials are units (that is, have multiplicative inverses). Indeed, for $a \in k$ with $a \neq 0$, since k is a field there is $a^{-1} \in k \subset k[x]$. Thus, certainly a is invertible in the polynomial ring $k[x]$. ♣

We can recycle the notation we used for cosets to write about ideals in a more economical fashion. For two subsets X, Y of a ring R , write

$$X + Y = \{x + y : x \in X, y \in Y\}$$

$$X \cdot Y = XY = \{ \text{finite sums } \sum_i x_i y_i : x_i \in X, y_i \in Y \}$$

Note that in the context of ring theory the notation $X \cdot Y$ has a different meaning than it does in group theory. Then we can say that an ideal I in a commutative ring R is an additive subgroup so that $RI \subset I$.

Proposition: Every ideal I in \mathbf{Z} is principal, that is, of the form $I = n \cdot \mathbf{Z}$. In particular, the integer n so that this is true is the least positive element of I unless $I = \{0\}$, in which case $n = 0$.

Proof: If $I = \{0\}$, then certainly $I = \mathbf{Z} \cdot 0$, and we're done. So suppose I is non-zero. Since I is closed under taking additive inverses, if I contains $x < 0$ then it also contains $-x > 0$. So a non-trivial ideal I does indeed contain some positive element. Let n be the least element of I . Let $x \in I$, and use the Division Algorithm to get $q, r \in \mathbf{Z}$ with $0 \leq r < n$ and

$$x = q \cdot n + r$$

Certainly qn is still in I , and then $-qn \in I$ also. Since $r = x - qn$, we conclude that $r \in I$. Since n was the smallest positive element of I , it must be that $r = 0$. Thus, $x = qn \in n \cdot \mathbf{Z}$, as desired. ♣

Proposition: Let k be a field. Let $R = k[x]$ be the ring of polynomials in one variable x with coefficients in k . Then every ideal I in R is principal, that is, is of the form $I = k[x] \cdot P(x)$ for some polynomial P . In particular, $P(x)$ is the monic polynomial of smallest degree in I , unless $I = \{0\}$, in which case $P(x) = 0$.

Proof: If $I = \{0\}$, then certainly $I = k[x] \cdot 0$, and we're done. So suppose I is non-zero. Suppose that $Q(x) = a_n x^n + \dots + a_0$ lies in I with $a_n \neq 0$. Since k is a field, there is an inverse a_n^{-1} . Then, since I is an ideal, the polynomial

$$P(x) = a_n^{-1} \cdot Q(x) = x^n + a_n^{-1} a_{n-1} x^{n-1} + \dots + a_n^{-1} a_0$$

also lies in I . That is, there is indeed a monic polynomial of lowest degree of any element of the ideal. Let $x \in I$, and use the Division Algorithm to get $Q, R \in k[x]$ with $\deg R < \deg P$ and

$$x = Q \cdot P + R$$

Certainly $Q \cdot P$ is still in I , and then $-Q \cdot P \in I$ also. Since $R = x - Q \cdot P$, we conclude that $R \in I$. Since P was the monic polynomial in I of smallest degree, it must be that $R = 0$. Thus, $x = Q \cdot P \in n \cdot k[x]$, as desired. ♣

Remark: The proofs of these two propositions can be abstracted to prove that every ideal in a Euclidean ring is principal.

Example: Let R be a commutative ring with unit 1, and fix two elements $x, y \in R$. Then

$$I = R \cdot x + R \cdot y = \{rx + sy : r, s \in R\}$$

is an ideal in R . This is checked as follows. First,

$$0 = 0 \cdot x + 0 \cdot y$$

so 0 lies in I . Second,

$$-(rx + sy) = (-r)x + (-s)y$$

so I is closed under inverses. Third, for two elements $rx + sy$ and $r'x + s'y$ in I (with $r, r', s, s' \in R$) we have

$$(rx + sy) + (r'x + s'y) = (r + r')x + (s + s')y$$

so I is closed under addition. Finally, for $rx + sy \in I$ with $r, s \in R$, and for $r' \in R$,

$$r' \cdot (rx + sy) = (r'r)x + (r's)y$$

so $R \cdot I \subset I$ as required. Thus, this type of I is indeed an ideal. The two elements x, y are the **generators** of I .

Example: Similarly, for fixed elements x_1, \dots, x_n of a commutative ring R , we can form an ideal

$$I = R \cdot x_1 + \dots + R \cdot x_n$$

Example: To construct new, larger ideals from old, smaller ideals we can proceed as follows. Let I be an ideal in a commutative ring R . Let x be an element of R . Then let

$$J = R \cdot x + I = \{rx + i : r \in R, i \in I\}$$

Let's check that J is an ideal. First

$$0 = 0 \cdot x + 0$$

so 0 lies in J . Second,

$$-(rx + i) = (-r)x + (-i)$$

so J is closed under inverses. Third, for two elements $rx + i$ and $r'x + i'$ in J (with $r, r' \in R$ and $i, i' \in I$) we have

$$(rx + i) + (r'x + i') = (r + r')x + (i + i')$$

so J is closed under addition. Finally, for $rx + i \in J$ with $r \in R, i \in I$, and for $r' \in R$,

$$r' \cdot (rx + i) = (r'r)x + (r'i)$$

so $R \cdot J \subset J$ as required. Thus, this type of set J is indeed an ideal.

Remark: In the case of rings such as \mathbf{Z} , where we know that every ideal is principal, the previous construction does not yield any more general type of ideal.

Remark: In some rings R , it is definitely the case that *not* every ideal is principal. That is, there are some ideals that cannot be expressed as $R \cdot x$. The simplest example is the following. Let

$$R = \{a + b\sqrt{-5} : a, b \in \mathbf{Z}\}$$

It is not hard to check that this is a ring. Let

$$I = \{x \cdot 2 + y \cdot (1 + \sqrt{-5}) : x, y \in R\}$$

With just a little bit of cleverness, one can show that this ideal is not principal. This phenomenon is closely related to the *failure of unique factorization* into primes in this ring. For example, we have two apparently different factorizations

$$2 \cdot 3 = 6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

(All the numbers 2, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ are "prime" in the naive sense that they can't be further factored in the ring R .) These phenomena are not of immediate relevance, but did provide considerable motivation in the historical development of algebraic number theory.

In rings R that are not necessarily commutative, there are *three different kinds* of ideals. A **left ideal** I is an additive subgroup so that $RI \subset I$, a **right ideal** I is an additive subgroup so that $IR \subset I$, and a **two-sided ideal** I is an additive subgroup so that $RIR \subset I$. Mostly we'll only care about ideals in *commutative* rings, so we can safely ignore this complication most of the time.

25.2 Ring homomorphisms

Quite analogous to *group homomorphisms*, ring homomorphisms are maps from one ring to another which preserve the ring structures.

A ring homomorphism $f : R \rightarrow S$ from one ring R to another ring S is a map so that, for all r, r' in R we have

$$\begin{aligned}f(r + r') &= f(r) + f(r') \\f(rr') &= f(r) f(r')\end{aligned}$$

That is, we would say that f *preserves* or *respects* both addition and multiplication.

A ring homomorphism which is a bijection is an **isomorphism**. Two rings which are isomorphic are construed as ‘the same’ for all ring-theoretic purposes.

As in the case of groups and group homomorphisms, we do not make an attempt to use different notations for the addition and multiplication in the two different rings R and S in this definition. Thus, more properly put, f converts *addition in R* into *addition in S* , and likewise multiplication.

Very much like the case of groups, the **kernel** of a ring homomorphism $f : R \rightarrow S$ is

$$\ker f = \{r \in R : f(r) = 0\}$$

where (implicitly) the latter 0 is the additive identity in S .

Example: The most basic example of a ring homomorphism is

$$f : \mathbf{Z} \rightarrow \mathbf{Z}/n$$

given by

$$f(x) = x\text{-mod-}n$$

The assertion that this f is a ring homomorphism is that

$$\begin{aligned}(x\text{-mod-}n) + (y\text{-mod-}n) &= (x + y)\text{-mod-}n \\f(1_R) \cdot s &= f(1_R) \cdot f(r) = f(1_R \cdot r) = f(r) = s\end{aligned}$$

Thus, $f(1_R)$ behaves like the unit in S . By the already prove *uniqueness* of units, it must be that $f(1_R) = 1_S$.

Now we prove that the kernel is an ideal. Let x be in the kernel, and $r \in R$. Then

$$f(rx) = f(r)f(x) = f(r) \cdot 0 = 0$$

since by now we’ve proven that in any ring the product of anything with 0 is 0. Thus, rx is in the kernel of f . And, for x, y both in the kernel,

$$f(x + y) = f(x) + f(y) = 0 + 0 = 0$$

That is, $x + y$ is again in the kernel. And $f(0) = 0$, so 0 is in the kernel. And for x in the kernel $f(-x) = -f(x) = -0 = 0$, so $-x$ is in the kernel. ♣

25.3 Quotient rings

Now we give a construction of new rings from old in a manner that includes as a special case the construction of \mathbf{Z}/n from \mathbf{Z} .

Let R be a commutative ring with unit 1. Let I be an ideal in R . The **quotient ring** R/I (“ R mod I ”) is defined to be the set of cosets

$$r + I = \{r + i : i \in I\}$$

We define operations of addition and multiplication on R/I by

$$(r + I) + (s + I) = (r + s) + I$$

$$(r + I) \cdot (s + I) = (r \cdot s) + I$$

The zero in this quotient will be $0_{R/I} = 0 + I$, and the unit will be $1_{R/I} = 1 + I$.

Example: The basic example is that \mathbf{Z}/n is the quotient ring \mathbf{Z}/I where $I = n \cdot \mathbf{Z}$.

But, just as we had to check that the operations of addition and multiplication in \mathbf{Z}/n were *well-defined*, we must do so here as well. The point is that the set $r + I$ typically can be named in several different ways, and we want the alleged addition and multiplication operations not to depend on the way the coset is *named*, but only on *what it is*. This is what well-definedness is about.

So suppose $r + I = r' + I$ and $s + I = s' + I$. That is, we have two cosets, each named in two possibly different ways. To prove well-definedness of addition we need to check that

$$(r + s) + I = (r' + s') + I$$

and to prove well-definedness of multiplication we must check that

$$(r \cdot s) + I = (r' \cdot s') + I$$

Since $r' + I = r + I$, in particular $r' = r' + 0 \in r + I$, so r' can be written as $r' = r + i$ for some $i \in I$. Likewise, $s' = s + j$ for some $j \in I$. Then

$$(r' + s') + I = (r + i + s + j) + I = (r + s) + (i + j + I)$$

The sum $k = i + j$ is an element of I . We claim that for any $k \in I$ we have $k + I = I$. Certainly since I is closed under addition, $k + I \subset I$. On the other hand, for any $x \in I$ we can write

$$x = k + (x - k)$$

with $x - k \in I$, so also $k + I \supset I$. Thus, indeed, $k + I = I$. Thus,

$$(r' + s') + I = (r + s) + I$$

which proves the well-definedness of addition in the quotient ring. Likewise, looking at multiplication:

$$(r' \cdot s') + I = (r + i) \cdot (s + j) + I = (r \cdot s) + (rj + si + I)$$

Since I is an ideal, rj and si are again in I , and then $rj + si \in I$. Therefore, as just observed in the discussion of addition, $rj + si + I = I$. Thus,

$$(r' \cdot s') + I = (r \cdot s) + I$$

and multiplication is well-defined.

The proofs that $0 + I$ is the zero and $1 + I$ is the unit are similar.

And in this situation the **quotient homomorphism**

$$q : R \rightarrow R/I$$

is the natural map

$$q(r) = r + I$$

In fact, the discussion just above proves

Proposition: For a commutative ring R and ideal I , the quotient map $R \rightarrow R/I$ is a ring homomorphism.



25.4 Maximal ideals and fields

Now we see how to make fields from by taking suitable quotients by maximal ideals. This is a fundamental construction.

Let R be a commutative ring with unit 1. An ideal M in R is **maximal** if $M \neq R$ and if for any other ideal I with $I \supset M$ it must be that $I = R$. That is, M is a maximal ideal if there is no ideal strictly larger than M (containing M) except R itself.

Proposition: For a commutative ring R with unit, and for an ideal I , the quotient ring R/I is a *field* if and only if I is a *maximal* ideal.

Proof: Let $x + I$ be a non-zero element of R/I . Then $x + I \neq I$, so $x \notin I$. Note that the ideal $Rx + I$ is therefore strictly larger than I . Since I was already maximal, it must be that $Rx + I = R$. Therefore, there are $r \in R$ and $i \in I$ so that $rx + i = 1$. Looking at this last equation modulo I , we have $rx \equiv 1 \pmod{I}$. That is, $r + I$ is the multiplicative inverse to $x + I$. Thus, R/I is a field.

On the other hand, suppose that R/I is a field. Let $x \in R$ but $x \notin I$. Then $x + I \neq 0 + I$ in R/I . Therefore, $x + I$ has a multiplicative inverse $r + I$ in R/I . That is,

$$(r + I) \cdot (x + I) = 1 + I$$

From the definition of the multiplication in the quotient, this is $rx + I = 1 + I$, or $1 \in rx + I$, which implies that the ideal $Rx + I$ is R . But $Rx + I$ is the smallest ideal containing I and x . Thus, there cannot be any proper ideal strictly larger than I , so I is maximal. 

25.5 Field extensions

Now we'll make the construction of the previous section more concrete, making 'bigger' fields by taking quotients of polynomial rings with coefficients in 'smaller' fields. This is a very basic procedure.

Let k be a field. Another field K containing k is called an **extension field** of k , and k is a **subfield** of K .

Theorem: Let k be a field and $P(x)$ an irreducible polynomial in $k[x]$ (other than the zero polynomial). Then the principal ideal $I = k[x] \cdot P(x)$ is *maximal*. Thus, the quotient ring $k[x]/I$ is a *field*. Further, the composite map

$$k \rightarrow k[x] \rightarrow k[x]/I$$

is *injective*, so we may consider the field k as a subset of the field $k[x]/I$. Last, let $\alpha = x + I$ be the image in $k[x]/I$ of the indeterminate x . Then (in the quotient $k[x]/I$)

$$P(\alpha) = 0$$

Last, any element $\beta \in k[x]/I$ can be *uniquely* expressed in the form

$$\beta = R(\alpha)$$

where R is a polynomial with coefficients in k and of degree strictly less than the degree of P .

Remark: The **degree** of the extension K of k is the degree of the polynomial P used in the construction.

Remark: In this situation, thinking of α as ‘existing’ now, and being a root of the equation $P(x) = 0$, we say that we have **adjoined** a root of $P(x) = 0$ to k , and write

$$k[\alpha] = k[x]/I$$

Remark: As a notational convenience, often a quotient

$$k[x]/k[x] \cdot P(x)$$

is written as

$$k[x]/P(x)$$

where it is meant to be understood that the quotient is by the *ideal* generated by $P(x)$. This is entirely consistent with the notation \mathbf{Z}/n for $\mathbf{Z}/\mathbf{Z} \cdot n$.

Remark: An element β of $k[x]/I$ expressed as a polynomial $R(\alpha)$ with R of degree less than the degree of P is **reduced**. Of course, since $k[x]/I$ is a ring, *any* polynomial $R(\alpha)$ in α gives something in $k[x]/I$. But everything can be expressed by a polynomial of degree less than that of P , and *uniquely* so. This is exactly analogous to the fact that every equivalence class in the quotient ring \mathbf{Z}/n has a unique representative among the integers reduced modulo n , namely $\{0, 1, 2, \dots, n-1\}$.

Proof: Let $J(x)$ be a polynomial not in the ideal $I = k[x] \cdot P(x)$. We want to show that the ideal $k[x] \cdot J(x) + I$ is $k[x]$, thereby proving the maximality of I . Since $P(x)$ is irreducible, the gcd of J and P is just 1. Therefore, by the Euclidean Algorithm in $k[x]$, there are polynomials A, B in $k[x]$ so that

$$A \cdot P + B \cdot J = 1$$

That is, $k[x] \cdot J(x) + I$ contains 1. Let $C(x), D(x)$ be polynomials so that

$$1 = C(x) \cdot J(x) + D(x) \cdot P(x)$$

Then for *any* polynomial $M(x)$ we have

$$M(x) = M(x) \cdot 1 = M(x) \cdot (C(x) \cdot J(x) + D(x) \cdot P(x)) = (M(x) \cdot C(x)) \cdot J(x) + (M(x) \cdot D(x)) \cdot P(x)$$

which lies in $k[x] \cdot J(x) + k[x] \cdot P(x)$. That is, $M(x)$ is in the ideal $k[x] \cdot J(x) + k[x] \cdot P(x)$, so the latter ideal is the whole ring $k[x]$. This proves the maximality of $k[x] \cdot J(x) + k[x] \cdot P(x)$.

Next, we show that the composite map

$$k \rightarrow k[x] \rightarrow k[x]/k[x] \cdot P(x)$$

is an injection. Let $I = k[x] \cdot P(x)$. The first map $k \rightarrow k[x]$ is the obvious one, which takes $a \in k$ to the “constant” polynomial a . Suppose $a, b \in k$ so that $a + I = b + I$. Then, by subtracting, $(a - b) + I = 0 + I$, which gives

$$a - b = (a - b) + 0 \in (a - b) + I = I$$

so $a - b \in I$.

Next, we prove that $P(\alpha) = 0$. Let $q : k[x] \rightarrow k[x]/I$ be the quotient homomorphism. Write out $P(x)$ as

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$$

To show that $P(\alpha) = 0$ in the quotient, we compute

$$\begin{aligned} P(\alpha) &= a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_2 \alpha^2 + a_1 \alpha + a_0 = a_n q(x)^n + a_{n-1} q(x)^{n-1} + \dots + a_2 q(x)^2 + a_1 \alpha + a_0 \\ &= q(a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0) = q(P(x)) \end{aligned}$$

since q is a ring homomorphism, and since the ‘constants’ in k are essentially unchanged in mapping to the quotient. Since $P(x) \in I$, the image $q(P(x))$ of it under q is 0. That is, we have proven that $P(\alpha) = 0$.

Finally, we prove that any element of the quotient $k[x]/I$ is uniquely expressible as a polynomial in $\alpha = x + I$, of degree less than the degree of P . Indeed, given $\beta \in k[x]/I$ there is some polynomial $J(x)$ so that $q(J(x)) = \beta$. Using the Division Algorithm for polynomials in one variable over a field, we have

$$J(x) = Q(x) \cdot P(x) + R(x)$$

where $\deg R < \deg P$. Then, under the homomorphism q we have

$$\beta = q(J(x)) = q(Q(x)) \cdot q(P(x)) + q(R(x)) = q(Q(x)) \cdot 0 + R(q(x)) = R(\alpha)$$

since $q(P(x)) = P(\alpha) = 0$, and of course using the ring homomorphism properties. This is the desired result. ♣

Corollary: When the field k is finite with q elements, for an irreducible polynomial $P(x)$ of degree n , the field extension $K = k[x]/P(x)$ with has q^n elements.

Proof: Let α be the image of x in K . We use the fact that every element of K has a unique expression as $R(\alpha)$ for a polynomial R of degree less than n . There are q choices for each of the n coefficients (for powers of α ranging from 0 to $n - 1$), so there are q^n elements altogether. ♣

Remark: A field extension $k[x]/P(x)$ with irreducible polynomial $P(x)$ is called **quadratic** if $P(x)$ is quadratic, **cubic** if $P(x)$ is cubic, **quartic** if $P(x)$ is quartic, **quintic** if $P(x)$ is quintic, etc.

25.6 Examples of field extensions

Now we’ll do some specific numerical examples of field extensions, using the set-up of the previous section.

Example: Let’s see how to ‘make’ the complex numbers \mathbf{C} as a **field extension** of the real number \mathbf{R} , *not* by presuming that there is a mysterious $\sqrt{-1}$ already existing “out there somewhere”.

First, let’s prove that $x^2 + 1 \in \mathbf{R}[x]$ is irreducible. Since the square of any real number is non-negative, the equation

$$x^2 + 1 = 0$$

has no roots in \mathbf{R} . Since the polynomial $x^2 + 1 \in \mathbf{R}[x]$ is quadratic, if it were to factor in $\mathbf{R}[x]$ it would have to factor into two linear factors (since the degree of the product is the sum of the degrees of the factors). But if $x^2 + 1$ had a linear factor then $x^2 + 1 = 0$ would have a root in \mathbf{R} , which it does not. Thus, in the polynomial ring $\mathbf{R}[x]$ the polynomial $x^2 + 1$ is irreducible, as claimed.

Let I be the ideal $I = \mathbf{R}[x] \cdot (x^2 + 1)$ generated by $x^2 + 1$ in $\mathbf{R}[x]$. Then, from above we know that $\mathbf{R}[x]/I$ is a field, inside which we can view \mathbf{R} as sitting. Also, we saw above that the image α of x in the quotient satisfies the equation $\alpha^2 + 1 = 0$.

We also showed that any element β of the extension is expressible uniquely in the form $\beta = a + b\alpha$ for $a, b \in \mathbf{R}$. Of course, we usually would write ‘ i ’ for the image of x in that extension field, rather than ‘ α ’.

Example: Let’s adjoin a square root of 2 to the field $\mathbf{Z}/5$. First, note that there is no a in $\mathbf{Z}/5$ so that $a^2 = 5$. Thus, the quadratic polynomial $x^2 - 2$ does not factor in $\mathbf{Z}/5[x]$ (since if it did it would have a root in $\mathbf{Z}/5$, which it doesn’t).

Let I be the ideal $I = \mathbf{Z}/5[x] \cdot (x^2 - 2)$ generated by $x^2 - 2$ in $\mathbf{Z}/5[x]$. Then, we know that $\mathbf{Z}/5[x]/I$ is a field, inside which we can view $\mathbf{Z}/5$ as sitting. Also, we saw above that the image α of x in the quotient satisfies the equation $\alpha^2 - 2 = 0$.

We also showed that any element β of the extension is expressible uniquely in the form $\beta = a + b\alpha$ for $a, b \in \mathbf{Z}/5$. Of course, we usually would write ‘ $\sqrt{2}$ ’ for the image of x in that extension field, rather than ‘ α ’.

Remark: Yes, these constructions might be viewed as anti-climactic, since the construction ‘makes’ roots of polynomials in a manner that seemingly is not as tangible as one would like. But in fact it’s *good* that the construction is fairly straightforward, since that partly means that *it works well*.

Example: Let’s adjoin a cube root of 2 to $\mathbf{Z}/7$. First, note that there is no cube root of 2 in $\mathbf{Z}/7$. (Check by brute force. Or, by noting that $\mathbf{Z}/7^\times$ is cyclic of order 6, from our basic facts about cyclic groups $\mathbf{Z}/7^\times$ will have only two third powers, which we can directly observe are ± 1 , so (by exclusion) 2 can’t be a cube.)

Thus, the cubic polynomial $x^3 - 2$ is irreducible in $\mathbf{Z}/7[x]$, since if it were *reducible* then it would have to have a linear factor, and then $x^3 - 2 = 0$ would have to have a root in $\mathbf{Z}/7$, which it doesn’t.

Let I be the ideal $I = \mathbf{Z}/7[x] \cdot (x^3 - 2)$. From this discussion, $\mathbf{Z}/7[x]/I$ is a field, and the image α of x in this quotient is a cube root of 2. And every element β of this field extension of $\mathbf{Z}/7$ can be uniquely expressed in the form

$$\beta = a_0 + a_1\alpha + a_2\alpha^2$$

25.7 Sums and products in field extensions

The addition, subtraction, and multiplication in field extensions are not hard to understand, because they are just what naturally arises from the corresponding operations on polynomials. In fact, a quotient $k[x]/I$ *inherits* its operations from $k[x]$, by the very construction.

Let k be a field, $P(x)$ an irreducible polynomial in $k[x]$, I the ideal generated by $P(x)$ in $k[x]$, and K the field extension $k[x]/I$ of k . Let α be the image of x in K . Let n be the degree of $P(x)$. Above we showed that any element of K can be expressed as a polynomial $R(\alpha)$ in α with $\deg < n$.

Addition of two elements

$$\beta = b_0 + b_1\alpha + b_2\alpha^2 + \dots + b_{n-2}\alpha^{n-2} + b_{n-1}\alpha^{n-1}$$

$$\gamma = c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_{n-2}\alpha^{n-2} + c_{n-1}\alpha^{n-1}$$

in the field extension K is the fairly obvious thing, as if we were adding polynomials:

$$\begin{aligned}\beta + \gamma &= b_0 + b_1\alpha + b_2\alpha^2 + \dots + b_{n-2}\alpha^{n-2} + b_{n-1}\alpha^{n-1} + c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_{n-2}\alpha^{n-2} + c_{n-1}\alpha^{n-1} \\ &= (b_0 + c_0) + (b_1 + c_1)\alpha + (b_2 + c_2)\alpha^2 + \dots + (b_{n-2} + c_{n-2})\alpha^{n-2} + (b_{n-1} + c_{n-1})\alpha^{n-1}\end{aligned}$$

Multiplication is somewhat messier, since the product of two polynomials of degree less than n is not reliably of degree less than n . In the present circumstance, somewhat more than in the case of the integers \mathbf{Z} , *reducing* polynomials modulo $P(x)$ via the Division Algorithm is more often necessary in order to understand what's going on.

So with β and γ as above, without trying to reduce mod P ,

$$\beta \cdot \gamma = \sum_{0 \leq i, j < n} a_i b_j \alpha^{i+j}$$

Of course, there is no simple general formula for what will be obtained if and when we reduce modulo P .

Example: In the field $K = \mathbf{Z}/5[\sqrt{2}]$ things are simple enough that we *can* get formulas for *reduced* products of two elements: let α be the image of x in the quotient $\mathbf{Z}/5[x]/(x^2 - 2)$. For $\alpha = a_0 + a_1\alpha$ and $\beta = b_0 + b_1\alpha$ in K ,

$$\alpha \cdot \beta = a_0 b_0 + (a_0 b_1 + a_1 b_0)\alpha + a_1 b_1 \alpha^2$$

In this simple example, the reduction occurs just in one step, since we know that $\alpha^2 = 2 \in \mathbf{Z}/5$. Therefore,

$$\alpha \cdot \beta = (a_0 b_0 + 2a_1 b_1) + (a_0 b_1 + a_1 b_0)\alpha$$

This is the general formula for multiplication in this field.

Example: In the field $k = \mathbf{Z}/7[\alpha]$ with $\alpha^3 = 2$ an explicit *formula* for the *reduced* product of $\beta = a_0 + a_1\alpha + a_2\alpha^2$ and $\gamma = b_0 + b_1\alpha + b_2\alpha^2$ will be messier, but still within reach if we want, and nothing counter-intuitive happens:

$$\begin{aligned}\beta \cdot \gamma &= (a_0 + a_1\alpha + a_2\alpha^2) \cdot (b_0 + b_1\alpha + b_2\alpha^2) \\ &= (a_0 b_0) + (a_0 b_1 + a_1 b_0)\alpha + (a_0 b_2 + a_1 b_1 + a_2 b_0)\alpha^2 + (a_1 b_2 + a_2 b_1)\alpha^3 + (a_2 b_2)\alpha^4\end{aligned}$$

Using the fact that $\alpha^3 = 2$, and that

$$\alpha^4 = (\alpha^3) \cdot \alpha = 2\alpha$$

this becomes

$$\beta \cdot \gamma = (a_0 b_0 + 2a_1 b_2 + 2a_2 b_1) + (a_0 b_1 + a_1 b_0 + 2a_2 b_2)\alpha + (a_0 b_2 + a_1 b_1 + a_2 b_0)\alpha^2$$

Remark: When the irreducible polynomial is anything other than something like the root-taking polynomials $x^n - a$, the *formula* won't be at all as simple as in this last example, but the underlying *procedure* is still as simple: **multiply and reduce**. The following two examples illustrate this:

Example: The polynomial $x^2 + x + 1$ has no linear factors in $\mathbf{Z}/2[x]$. Let α be a root of $x^2 + x + 1 = 0$ in the extension field $\mathbf{Z}/2[x]/(x^2 + x + 1)$. Thus, rather than knowing that α raised to some power is an element of $\mathbf{Z}/2$, instead from $\alpha^2 + \alpha + 1 = 0$ we have

$$\alpha^2 = -\alpha - 1 = \alpha + 1$$

(since $-1 = +1$ in $\mathbf{Z}/2$). Then an explicit *formula* for the reduced product of $\beta = b_0 + b_1\alpha$ and $\gamma = c_0 + c_1\alpha$. It is

$$\beta \cdot \gamma = (b_0 + b_1\alpha) \cdot (c_0 + c_1\alpha) = (b_0 c_0) + (b_1 c_0 + b_0 c_1)\alpha + (b_1 c_1)\alpha^2$$

$$= (b_o c_o) + (b_1 c_o + b_o c_1)\alpha + (b_1 c_1)(\alpha + 1) = (b_o c_o + b_1 c_1) + (b_1 c_o + b_o c_1 + b_1 c_1)\alpha$$

This formula is not really so helpful, since it is too complicated to really allow intuitive access. Yet what we're actually doing is *numerically* quite straightforward: **multiply and reduce mod $P(x)$** .

Example: Consider the polynomial $x^4 + x^3 + x^2 + x + 1$ in $\mathbf{Z}/2[x]$. First we want to prove that it is irreducible. Again, the equation

$$x^4 + x^3 + x^2 + x + 1 = 0$$

has no roots in $\mathbf{Z}/2$, so there is no linear factor. However, since it is of degree larger than 3, it *might* factor in some way without having a *linear* factor, thereby *maybe* factoring without $x^4 + x^3 + x^2 + x + 1 = 0$ having a root. In this instance, what could conceivably happen is that

$$x^4 + x^3 + x^2 + x + 1 = (\text{irreducible quadratic}) \cdot (\text{irreducible quadratic})$$

But this is still within reach of essentially brute-force computation: suppose

$$x^4 + x^3 + x^2 + x + 1 = (x^2 + ax + 1) \cdot (x^2 + bx + 1)$$

for some $a, b \in \mathbf{Z}/2$. Note that we can be sure that the highest and lowest coefficients of the quadratic factors are 1, rather than 0, since the highest and lowest factors of $x^4 + x^3 + x^2 + x + 1$ are 1 rather than 0. Multiplying out, we would have

$$x^4 + x^3 + x^2 + x + 1 = x^4 + (a+b)x^3 + (ab)x^2 + (a+b)x + 1$$

(since $2 = 0$). Thus, comparing the x^2 coefficients, we would have $a = b = 1$. But then, comparing the x^4 and x coefficients, it is impossible to have $a + b = 1$. That is, there are no such quadratic factors in $\mathbf{Z}/2[x]$. Thus, in fact $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbf{Z}/2[x]$.

Let α be a root of $x^4 + x^3 + x^2 + x + 1 = 0$ in the extension field $K = \mathbf{Z}/2[x]/(x^4 + x^3 + x^2 + x + 1)$. Thus, rather than knowing that α raised to some power is an element of $\mathbf{Z}/2$, instead, from $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$ we have

$$\alpha^5 = -\alpha^3 - \alpha^2 - \alpha - 1 = \alpha^3 + \alpha^2 + \alpha + 1$$

(since $-1 = +1$ in $\mathbf{Z}/2$). And of course

$$\begin{aligned} \alpha^6 &= (\alpha^5) \cdot \alpha = (\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)\alpha \\ &= \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha = (\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) + \alpha^4 + \alpha^3 + \alpha^2 + \alpha = 1 \end{aligned}$$

This is not so surprising since, after all,

$$(x^4 + x^3 + x^2 + x + 1) \cdot (x - 1) = x^5 - 1$$

Then an explicit *formula* for the reduced product of $\beta = b_o + b_1\alpha + b_2\alpha^2 + b_3\alpha^3$ and $\gamma = c_o + c_1\alpha + c_2\alpha^2 + c_3\alpha^3$ is the hopelessly messy expression

$$\begin{aligned} \beta \cdot \gamma &= (b_o c_o) + (b_1 c_o + b_o c_1)\alpha + (b_2 c_o + b_1 c_1 + b_o c_2)\alpha^2 + (b_3 c_o + b_2 c_1 + b_1 c_2 + b_o c_3)\alpha^3 \\ &\quad + (b_3 c_1 + b_2 c_2 + b_1 c_3)\alpha^4 + (b_3 c_2 + b_2 c_3)\alpha^5 + (b_3 c_3)\alpha^6 \\ &= (b_o c_o) + (b_1 c_o + b_o c_1)\alpha + (b_2 c_o + b_1 c_1 + b_o c_2)\alpha^2 + (b_3 c_o + b_2 c_1 + b_1 c_2 + b_o c_3)\alpha^3 \\ &\quad + (b_3 c_1 + b_2 c_2 + b_1 c_3)\alpha^4 + (b_3 c_2 + b_2 c_3)(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) + (b_3 c_3) \cdot 1 \\ &= (b_o c_o + (b_3 c_2 + b_2 c_3) + b_3 c_3) + (b_1 c_o + b_o c_1 + (b_3 c_2 + b_2 c_3))\alpha + (b_2 c_o + b_1 c_1 + b_o c_2 + (b_3 c_2 + b_2 c_3))\alpha^2 \\ &\quad + (b_3 c_o + b_2 c_1 + b_1 c_2 + b_o c_3 + (b_3 c_2 + b_2 c_3))\alpha^3 + (b_3 c_1 + b_2 c_2 + b_1 c_3 + (b_3 c_2 + b_2 c_3))\alpha^4 \end{aligned}$$

Yet the **numerical process** is not so complicated. For example, to find the product of

$$\beta = A(\alpha) = \alpha^3 + \alpha + 1$$

and

$$\gamma = B(\alpha) = \alpha^3 + \alpha^2 + 1$$

thinking of $A(\alpha)$ and $B(\alpha)$ as polynomials evaluated at α , we first do the obvious **multiplication**

$$\begin{aligned} \beta \cdot \gamma &= (\alpha^3 + \alpha + 1) \cdot (\alpha^3 + \alpha^2 + 1) \\ &= \alpha^6 + \alpha^5 + \alpha^4 + 3 \cdot \alpha^3 + \alpha^2 + \alpha + 1 \\ &= \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 \end{aligned}$$

To **reduce** is just to **divide-with-remainder** by $P(x)$:

$$(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) - (x^2)(x^4 + x^3 + x^2 + x + 1) = x + 1$$

Therefore,

$$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = \alpha + 1$$

Altogether, we have computed

$$(\alpha^3 + \alpha + 1) \cdot (\alpha^3 + \alpha^2 + 1) = \alpha + 1$$

25.8 Multiplicative inverses in field extensions

By contrast to addition and multiplication, the procedure for computing multiplicative inverses is less obvious. But, in fact, computation of multiplicative inverses in finite fields can be done quite efficiently using either the Euclidean Algorithm in *polynomial rings* (as we used earlier to compute inverses in \mathbf{Z}/n). There is another algorithm which takes advantage of the *finiteness* of the fields, but which is relatively very slow, as described below.

Note that in an abstract and indirect way we know that any non-zero element of K does *have* an inverse, since we have already proven that K is indeed a field. The problem is to be able to *compute* the inverse reasonably.

In a field extension $K = k[x]/P(x)$ with $P(x)$ irreducible in $k[x]$, let α be the image of x , so α is a root of the equation $P(x) = 0$ in K . Given a polynomial J , to find the multiplicative inverse of $J(\alpha)$ proceed as follows. First, we must be assuming that $J(\alpha) \neq 0$ in K , or else it *shouldn't* have an inverse in K anyway. That is, the polynomial $P(x)$ does not divide $J(x)$. Since $P(x)$ is *irreducible*, this means that the *gcd* of $P(x)$ and $J(x)$ is 1. Therefore, when we run the Euclidean Algorithm ('forward') with $P(x)$ and $J(x)$, at some point we will reach

$$(\dots) - (\dots) \cdot (\dots) = c$$

with a non-zero constant $c \in k$. Running the Euclidean Algorithm 'backward' yields polynomials $S_o(x), T_o(x)$ so that

$$S_o(x)P(x) + T_o(x)J(x) = c$$

This isn't quite what we want, since we want the right-hand side to be 1. But since c is non-zero, it has a multiplicative inverse c^{-1} in k , so

$$c^{-1}S_o(x)P(x) + c^{-1}T_o(x)J(x) = 1$$

Thus, letting

$$S(x) = c^{-1}S_o(x) \quad T(x) = c^{-1}T_o(x)$$

Then

$$S(x)P(x) + T(x)J(x) = 1$$

Looking at this modulo $P(x)$, we find

$$T(x) \cdot J(x) = 1 \pmod{P(x)}$$

Therefore,

$$T(\alpha) \cdot J(\alpha) = 1$$

. This is completely analogous to our procedure for computing multiplicative inverses in \mathbf{Z}/n .

There is an additional approach which is feasible for relatively small **finite fields**. It is much worse than the Euclidean Algorithm approach, however. Let k be a finite field with q elements, let $P(x)$ be irreducible of degree n in $k[x]$, and let $K = k[x]/P(x)$. We saw above that K has q^n elements. We proved earlier (when thinking about primitive roots) that the group K^\times is *cyclic*. Since K^\times is just K with 0 removed, it has $q^n - 1$ elements. Therefore, for any $\beta \in K^\times$, we have

$$\beta^{q^n - 1} = 1$$

since by Lagrange's theorem the order of any element divides the order of the whole group. This is the same argument that proves Euler's theorem from Lagrange's theorem. Then

$$\beta \cdot (\beta^{q^n - 2}) = \beta^{q^n - 1} = 1$$

That is, for any $\beta \in K^\times$, the **multiplicative inverse** of β in K is $\beta^{q^n - 2}$.

Remark: Even when q^n is a bit large, this power of β can be reasonably computed by the fast exponentiation algorithm, but for large $q^n - 1$ this approach becomes much worse than the Euclidean Algorithm approach.

Example: Let's compute the multiplicative inverse of $\alpha^3 + \alpha + 1$ where α is the image of x in the field extension $K = \mathbf{Z}/2[x]/P(x)$ where $P(x) = x^4 + x^3 + x^2 + x + 1$. First, we run the Euclidean Algorithm:

$$\begin{aligned} (x^4 + x^3 + x^2 + x + 1) - (x + 1)(x^3 + x + 1) &= x \\ (x^3 + x + 1) - (x^2 + 1)(x) &= 1 \end{aligned}$$

Running this 'backward', we have

$$\begin{aligned} 1 &= (x^3 + x + 1) - (x^2 + 1)(x) \\ &= (x^3 + x + 1) - (x^2 + 1)((x^4 + x^3 + x^2 + x + 1) - (x + 1)(x^3 + x + 1)) \\ &= (1 + (x^2 + 1)(x + 1))(x^3 + x + 1) - (x^2 + 1)(x^4 + x^3 + x^2 + x + 1) \\ &= (x^3 + x^2 + x)(x^3 + x + 1) + (x^2 + 1)(x^4 + x^3 + x^2 + x + 1) \end{aligned}$$

Thus, $x^3 + x^2 + x$ is an inverse of $x^3 + x + 1$ modulo $P(x)$, so $\alpha^3 + \alpha^2 + \alpha$ is the inverse of $\alpha^3 + \alpha + 1$ in K .

In this example, since $\mathbf{Z}/2$ has 2 elements, and $P(x)$ is of degree 4, the extension field K has 2^4 elements. Thus, for any $\beta \in K^\times$,

$$1 = \beta^{2^4 - 1} = \beta^{15}$$

Thus, as observed above, for any β in K^\times ,

$$\beta^{-1} = \beta^{14}$$

Remark: It is noteworthy that in the fast exponentiation algorithm, squaring polynomials with coefficients in a field of *characteristic 2* (that is, where $2 = 0$) is unusually easy, since the binomial coefficient

$$\binom{2}{1} = 2$$

so

$$(x + y)^2 = x^2 + 2xy + y^2 = x^2 + 0 \cdot xy + y^2 = x^2 + y^2$$

Generally, with coefficient in such a field,

$$(a_0 + a_1x + a_2x^2 + a_3x^3 + \dots + a_{n-1}x^{n-1} + a_nx^n)^2 = a_0^2 + a_1^2x^2 + a_2^2x^4 + a_3^2x^6 + \dots + a_{n-1}^2x^{2(n-1)} + a_n^2x^{2n}$$

This makes roughly half of the steps in the fast exponentiation algorithm very easy.

Example: Let $k = \mathbf{Z}/13$, $P(x) = x^3 - 2$, $K = k[x]/P(x)$, let α be the image of x in K , and find the multiplicative inverse of $\alpha^2 + \alpha + 2$. Note that 2 is not a cube mod 13, so this cubic polynomial is irreducible. Note that in this example the fast exponentiation approach would require that we compute the $(13^3 - 2)^{\text{th}}$ ($= 2196^{\text{th}}$) power of $x^2 + x + 1$, which would take roughly 16 steps. This is more burdensome than the Euclidean Algorithm approach.

Running the Euclidean Algorithm forward:

$$\begin{aligned} (x^3 - 2) - (x - 1)(x^2 + x + 2) &= -x \\ (x^2 + x + 2) - (-x - 1)(-x) &= 2 \end{aligned}$$

Going backwards, we obtain

$$\begin{aligned} 2 &= (x^2 + x + 2) - (-x - 1)(-x) = (x^2 + x + 2) + (x + 1)(-x) \\ &= (x^2 + x + 2) + (x + 1)((x^3 - 2) - (x - 1)(x^2 + x + 2)) \\ &= (1 - (x + 1)(x - 1))(x^2 + x + 2) + (x + 1)(x^3 - 2) \\ &= (-x^2)(x^2 + x + 2) + (x + 1)(x^3 - 2) \end{aligned}$$

Then multiply through by the multiplicative inverse of 2 in $\mathbf{Z}/13$, namely 7, to obtain

$$1 = 7 \cdot (-x^2)(x^2 + x + 2) + 7 \cdot (x + 1)(x^3 - 2)$$

Looking at this modulo $x^3 - 2$, we obtain

$$1 = (-7x^2)(x^2 + x + 2) \pmod{x^3 - 2}$$

Since $-7 = 6 \pmod{13}$, we can also write

$$1 = (6x^2)(x^2 + x + 2) \pmod{x^3 - 2}$$

Therefore,

$$(\alpha^2 + \alpha + 2)^{-1} = 6\alpha^2$$

#25.221 Verify that $x^2 - x + 1$ is an *irreducible* polynomial in $\mathbf{F}_2[x]$ where $\mathbf{F}_2 = \mathbf{Z}/2$.

#25.222 Verify that $x^3 - x + 1$ is an *irreducible* polynomial in $\mathbf{F}_3[x]$ where $\mathbf{F}_3 = \mathbf{Z}/3$.

#25.223 In the field $\mathbf{Z}/2[x]/(x^2 + x + 1)$ let α be the image of x , and compute (in reduced form) $(1 + \alpha)^2$.

#25.224 In the field $\mathbf{Z}/2[x]/(x^2 + x + 1)$ let α be the image of x , and compute (in reduced form) $(1 + \alpha)^{-1}$.

#25.225 In the field $\mathbf{Z}/3[x]/x^3 - x + 1$ let α be the image of x , and compute (in reduced form) $(1 + \alpha)(2 + \alpha - \alpha^2)$.

#25.226 In the field $\mathbf{Z}/2[x]/(x^2 + x + 1)$ let α be the image of x , and compute (in reduced form) $(1 + \alpha - \alpha^2)^{-1}$.

#25.227 *Fermat's Little Theorem:* Show that for prime p and integer x , we have $x^p \equiv x \pmod{p}$.

#25.228 Show that for prime p the polynomial $x^p - x$ with coefficients in \mathbf{Z}/p factors as

$$x^p - x = x(x - 1)(x - 2)(x - 3) \dots (x - (p - 2))(x - (p - 1))$$

#25.229 Show that there are 27 different numbers $x \pmod{7 \cdot 13 \cdot 19}$ so that $x^3 \equiv -1 \pmod{7 \cdot 13 \cdot 19}$. (*Hint:* Notice that the question didn't really ask you to *find* all of them. It might be sensible to find the three solutions of the congruence separately modulo each of 7, 13, and 19, and then worry about solving *systems* of congruences.)

#25.230 Let k be any field, and suppose that P is a monic polynomial in $k[x]$ which factors as

$$P(x) = (x - r_1)(x - r_2) \dots (x - r_n)$$

with all the roots $r_i \in k$. Show that $P(x)$ has a *double* root if and only if $\gcd(P, P')$ is a polynomial of positive degree, where P' is the *derivative* of P in the usual sense! (*Thus, we can detect the presence of double roots without actually having to solve equations!*)

#25.231 Let p be a prime number, and let a be a non-zero element in \mathbf{Z}/p . Show that $x^p - x + a = 0$ has no root in \mathbf{Z}/p .

#25.232 (*) Let k be any field. Prove that there are infinitely many distinct *irreducible* ('prime') polynomials in $k[x]$. (*Hint:* Imitate Euclid's proof of the infinitude of prime *numbers*.)

26. Linear Congruences

We have already seen that the Euclidean Algorithm gives a systematic procedure (an *algorithm*) to solve the congruence

$$ax \equiv 1 \pmod{m}$$

for x , given a, m when $\gcd(a, m) = 1$. Specifically, the Euclidean Algorithm applied to a and m yields integers x, y so that

$$ax + my = 1$$

Looking at this equation modulo m , we have $ax - 1 = -my$, so $ax - 1$ is a multiple of m , and $ax \equiv 1 \pmod{m}$.

A little more generally, let's look at the congruence

$$ax \equiv b \pmod{m}$$

which we are to solve for x , given a, b, m . *First, let's suppose for simplicity that $\gcd(a, m) = 1$.* Then we can find x_o so that

$$ax_o \equiv 1 \pmod{m}$$

Then, multiplying both sides of this congruence by b , we obtain

$$ax_o b \equiv b \pmod{m}$$

Thus, $x_o b$ is a solution to the congruence.

If $\gcd(a, m) > 1$, the issue of *solvability* of the congruence is a little more delicate. In particular, depending on the circumstances, *there may or may not be a solution*.

As a second case, let's consider the situation that $\gcd(a, m) > 1$ and that

$$\gcd(a, m) \nmid b$$

Then there's no solution to the congruence

$$ax \equiv b \pmod{m}$$

To see this, write $d = \gcd(a, m)$, for brevity. Suppose x were a solution to the congruence. Then $ax - b = km$ for some integer k . Rearranging a little, we have

$$ax - km = b$$

Now $d|a$ and $d|m$, so d divides the left-hand side of this equality. But this is impossible, since $d \nmid b$. Thus, there could not have been any such solution x !

So it remains to consider the case that $\gcd(a, m) > 1$ and that

$$\gcd(a, m) | b$$

In this case there *is* a solution, and the method to find it is by reducing to the first, simplest case. Let $d = \gcd(a, m)$ for brevity. If we *had* a solution x to the congruence $ax \equiv b \pmod{m}$, then for some integer k we have

$$ax - b = km$$

From this, by dividing through by d , we obtain

$$\frac{a}{d}x - \frac{b}{d} = k\frac{m}{d}$$

where it is important that all the fractions here are really *integers*. That is, a solution x to

$$ax \equiv b \pmod{m}$$

is also a solution to

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

Going in the other direction, suppose that x is a solution to the congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

Then multiply through by d to obtain

$$ax \equiv b \pmod{m}$$

Thus, what we've found out is that solutions to $ax \equiv b \pmod{m}$ are in one-to-one correspondence with solutions to $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

Now when we divide through by $\gcd(a, m)$ we have managed to return to the situation already treated, since

$$\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = \gcd\left(\frac{a}{\gcd(a, m)}, \frac{m}{\gcd(a, m)}\right) = 1$$

and we can use the Euclidean Algorithm to solve this.

Finally, we note that these congruences are all **linear**, meaning that there is no x^2 term, no x^3 term, etc., that is, nothing more complicated than 'constants' and constant multiples of x occurring in the congruences.

#26.233 Solve $5x \equiv 1 \pmod{101}$.

#26.234 Solve $5x \equiv 17 \pmod{101}$.

#26.235 Solve $41x \equiv 19 \pmod{103}$.

#26.236 Solve $5x \equiv 105 \pmod{1000}$.

#26.237 Solve $15x \equiv 105 \pmod{1000}$.

27. Systems of Linear Congruences

Now let's look at *systems* of linear congruences. There are some similarities to the more elementary discussion of systems of linear *equations*, but there are critical differences, as well. Part of the issue is clarified if one knows about Sun Ze's theorem (Chinese Remainder Theorem), since that theorem explains that certain otherwise peculiar steps below are in fact completely reasonable.

To start with, let's take the smallest non-trivial systems, of the form

$$\begin{aligned}ax &\equiv b \pmod{m} \\cx &\equiv d \pmod{n}\end{aligned}$$

Notice right away that there are *two* congruences but just one *unknown*, which would lead to non-solvability immediately in the case of *equations*. But systems of congruences behave slightly differently. Our only concession is: **We'll only consider the case that the moduli m and n are relatively prime, that is, that $\gcd(m, n) = 1$.**

By our previous discussion of a *single* congruence, we know how to solve (or detect non-solvability of) the *individual* congruences

$$ax \equiv b \pmod{m}$$

and

$$cx \equiv d \pmod{n}$$

Certainly if either of these separate congruences has *no* solution then there is no solution for both *together*, so let's just contemplate the situation that *both do have* solutions: let x_1 be a solution to $ax \equiv b \pmod{m}$ and let x_2 be a solution to $cx \equiv d \pmod{n}$. The question is *how to get from the separate solution x_1, x_2 to a simultaneous solution x* . This is where Sun Ze's theorem (Chinese Remainder Theorem) comes in. But, in fact, we need a *computationally effective* version, so we use the *Euclidean algorithm*.

Then, using the Euclidean algorithm again, there are integers s, t so that

$$sm + tn = 1$$

since we supposed that $\gcd(m, n) = 1$. And this can be rearranged to

$$tn = 1 - sm$$

for example. **Here comes the trick:** the claim is that **the single congruence**

$$x_o = x_1(tn) + x_2(sm) \pmod{mn}$$

is equivalent to (has the same set of solutions) as the *system* of congruences.

Let's check: modulo m , we have

$$\begin{aligned}ax_o &\equiv a(x_1(tn) + x_2(sm)) \pmod{m} \equiv a(x_1(tn) + 0) \pmod{m} \\ &\equiv (ax_1)(tn) \pmod{m} \equiv (ax_1)(1 - sm) \pmod{m} \\ &\equiv (ax_1)(1) \pmod{m} \equiv ax_1 \equiv b \pmod{m}\end{aligned}$$

The discussion of the congruence modulo n is nearly identical, with roles reversed. Thus, anything congruent to this x_o modulo mn is a solution to the system.

On the other hand, suppose x is a solution to the system, and let's prove that it is congruent to x_o modulo mn . Since $ax \equiv b \pmod{m}$ and $ax \equiv b \pmod{n}$, we have

$$a(x - x_o) \equiv b - b \equiv 0 \pmod{m}$$

Similarly,

$$c(x - x_o) \equiv d - d \equiv 0 \pmod{n}$$

That is, both m and n divide $x - x_o$. Since m and n are relatively prime, we can conclude that mn divides $x - x_o$, as desired.

The latter principle, that if m and n are relatively prime and if both divide y then mn divides y , merits some reflection! How would a person prove it, for example?

Note that solving the individual congruences uses the Euclidean Algorithm, as does the process of sticking the solutions together via the goofy formula above.

For example, to solve the system

$$\begin{aligned} 3x &\equiv 2 \pmod{11} \\ 5x &\equiv 7 \pmod{13} \end{aligned}$$

we first solve the congruences separately: using the Euclidean Algorithm (whose execution we omit here!) we find out that

$$3 \cdot 8 \equiv 2 \pmod{11}$$

and

$$5 \cdot 4 \equiv 7 \pmod{13}$$

To 'glue' these solutions together, we execute the Euclidean Algorithm again, to find

$$6 \cdot 11 - 5 \cdot 13 = 1$$

Thus, the single congruence

$$x \equiv 8(-5 \cdot 13) + 4(6 \cdot 11) \pmod{11 \cdot 13}$$

is equivalent to the system. In particular, this gives a solution

$$x = -8 \cdot 5 \cdot 13 + 4 \cdot 6 \cdot 11 = 784$$

Now, quite generally, consider a system

$$\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ a_3x &\equiv b_3 \pmod{m_3} \\ &\dots \\ a_nx &\equiv b_n \pmod{m_n} \end{aligned}$$

We'll only consider the scenario that each pair of m_i and m_j are relatively prime (for $i \neq j$). We solve it in steps: first, just look at the subsystem

$$\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \end{aligned}$$

and use the method above to turn this into a single (equivalent!) congruence of the form

$$x \equiv c_2 \pmod{m_1m_2}$$

Then look at the system

$$\begin{aligned}x &\equiv c_2 \pmod{m_1 m_2} \\ a_2 x &\equiv b_2 \pmod{m_3}\end{aligned}$$

and use the method above to combine these two congruences into a single equivalent one, say

$$x \equiv c_3 \pmod{m_1 m_2 m_3}$$

and so on.

#27.238 Solve the *two* simultaneous congruences:

$$\begin{aligned}7x &\equiv 1 \pmod{15} \\ 3x &\equiv 2 \pmod{17}\end{aligned}$$

#27.239 Solve the *three* simultaneous congruences

$$\begin{aligned}4x &\equiv 1 \pmod{15} \\ 6x &\equiv 2 \pmod{17} \\ 18x &\equiv 3 \pmod{19}\end{aligned}$$

28. Abstract Sun Ze Theorem

The goal of this section is to prove a theorem which includes as a very special case an assertion about solving several congruences simultaneously. The concrete version of this theorem is very old, and is attributed to Sun Ze (with ambiguous spelling). It is also sometimes called the “Chinese Remainder Theorem”. So what we prove here is an **abstract Sun Ze theorem**.

Let R be a commutative ring, and I an ideal in it. Extending the notation for congruences of ordinary integers, we may write

$$x \equiv y \pmod{I}$$

if $x - y \in I$. As discussed repeatedly earlier, this is equivalent to the assertion that $x + I = y + I$, as elements of the quotient R/I . Thus, our general discussion about quotient rings subsumes the earlier discussion of integers-mod- m . Even though we can talk about the images of elements in the quotient, it is occasionally useful to have the congruence notation available.

As another item of notation, for two ideals I, J of a commutative ring R , let $I \cdot J$ be the ideal consisting of all finite sums of products $i \cdot j$ where $i \in I$ and $j \in J$. That is, every element of $I \cdot J$ is expressible as

$$i_1 j_1 + i_2 j_2 + \dots + i_n j_n$$

with all the i_ℓ 's in I and all the j_ℓ 's in J . The number n of summands can vary. *Note that this is a different notational convention than the notation $X \cdot Y$ used for subsets. It is necessary to use context to determine which is meant, the “ideal” multiplication or the “subset” multiplication.*

The following lemma relates this construct to the more down-to-earth *intersection* of ideals:

Lemma: Let I, J be two ideals in a commutative ring R , with a unit ‘1’. If $I + J = R$ then $I \cdot J = I \cap J$.

Proof: On one hand, since

$$I \cdot J \subset I \cdot R = I$$

and

$$I \cdot J \subset R \cdot J = J$$

it follows that $I \cdot J \subset I \cap J$. On the other hand, take $h \in I \cap J$. Since $I + J = R$ and R has a unit, there are $i \in I$ and $j \in J$ so that $i + j = 1$. Then

$$h = h \cdot 1 = h \cdot (i + j) = h \cdot i + h \cdot j \in J \cdot i + I \cdot j$$

since h lies in both I and J . Thus,

$$h \in h \cdot i + h \cdot j \in J \cdot i + I \cdot j \subset J \cdot I + I \cdot J = I \cdot J$$

This proves the other inclusion, thereby giving the desired equality. *Done.*

Theorem: (*Sun Ze*) Let R be a commutative ring with a unit '1'. Let I and J be two ideals in R , so that

$$I + J = R$$

Then, for any two elements $a, b \in R$ there is $x \in R$ so that

$$x \equiv a \pmod{I} \quad \text{and} \quad x \equiv b \pmod{J}$$

In particular, if $i \in I$ and $j \in J$ are the elements so that $i + j = 1$, then

$$x = aj + bi$$

is an element of R satisfying both congruence conditions. Further, if x' is another element of R also satisfying $x' \equiv a \pmod{I}$ and $x' \equiv b \pmod{J}$, then $x \equiv x' \pmod{I \cdot J}$, where $I \cdot J$ is the ideal consisting of all finite sums of products $u \cdot v$ where $u \in I$ and $v \in J$. That is, the solution to the system $x \equiv a \pmod{I}$, $x \equiv b \pmod{J}$ is unique modulo $I \cdot J$.

Proof: It certainly suffices to check that the formula $x = aj + bi$ does what is claimed.

On one hand, since $i \in I$ and $j \in J$, $i \equiv 0 \pmod{I}$ and $j \equiv 0 \pmod{J}$. Thus, from $i + j = 1$, certainly $i \equiv 1 \pmod{J}$, and also $j \equiv 1 \pmod{I}$. Therefore,

$$aj + bi \equiv a \cdot 1 + b \cdot 0 \pmod{I} \equiv a \pmod{I}$$

and symmetrically

$$aj + bi \equiv a \cdot 0 + b \cdot 1 \pmod{J} \equiv b \pmod{J}$$

as desired.

For the uniqueness assertion, suppose that x, x' are two solutions. Then $x - x' \equiv a - a \equiv 0 \pmod{I}$ and similarly $x - x' \equiv b - b \equiv 0 \pmod{J}$. That is, $x - x' \in I \cap J$. The lemma above proves that $I \cap J = I \cdot J$ in this situation, so $x - x' \in I \cdot J$. *Done.*

Corollary: Let R be a commutative ring with unit '1', and let I_1, \dots, I_n be ideals so that for any two distinct indices k, ℓ we have

$$I_k + I_\ell = R$$

Then, for any elements a_1, \dots, a_n , there is $x \in R$ so that for every index k we have

$$x \equiv a_k \pmod{I_k}$$

And this x is uniquely determined modulo

$$I_1 \cdot I_2 \cdot \dots \cdot I_n = I_1 \cap I_2 \cap \dots \cap I_n$$

Proof: This will follow from the theorem by induction: the theorem treats $n = 2$, and the case $n = 1$ is trivial. By induction, we can find an x_o so that $x_o \equiv b_\ell \pmod{I_\ell}$ for $1 \leq \ell \leq n - 1$. And this x_o is uniquely determined modulo $I_1 \cdot \dots \cdot I_{n-1}$.

Thus, consider the system of two congruences

$$x \equiv x_o \pmod{I_1 \cdot \dots \cdot I_{n-1}}$$

$$x \equiv b_n \pmod{I_n}$$

If we can show that

$$I_1 \cdot \dots \cdot I_{n-1} + I_n = R$$

then we can simply apply the theorem again, proving the corollary.

For $1 \leq \ell \leq n-1$, take $i_\ell \in I_\ell$ and $j_\ell \in I_n$ so that $i_\ell + j_\ell = 1$. Then

$$\begin{aligned} 1 &= 1 \cdot 1 \cdot \dots \cdot 1 = (i_1 + j_1) \cdot (i_2 + j_2) \cdot \dots \cdot (i_{n-1} + j_{n-1}) \\ &= i_1 i_2 \dots i_{n-1} + (\text{all other terms}) \end{aligned}$$

simply by multiplying out the $n-1$ factors of the form $i_\ell + j_\ell$. All the terms inside the large parentheses have a factor of j_ℓ for some ℓ . Thus, each summand inside the large parentheses lies inside I_n . That is, the expression inside the parentheses lies in I_n . And the first term certainly lies inside $I_1 \cdot \dots \cdot I_{n-1}$. This proves what was necessary for the corollary to follow from the theorem. *Done.*

#28.240 Prove from first principles that for an ideal I in a ring R that

$$x \sim y \quad \text{if and only if} \quad x - y \in I$$

is an equivalence relation.

#28.241 For ideals I, J in a commutative ring R , prove that the ideal $I \cdot J$ (consisting of all finite sums of products $i \cdot j$ with $i \in I$ and $j \in J$) really is an ideal.

#28.242 Give an example to show that (for two ideals I, J in a commutative ring) without the condition $I + J = R$ it can be that $I \cdot J$ is strictly smaller than $I \cap J$.

#28.243 Give an example of three ideals I, J, K in the ring $R = \mathbf{Z}$ so that $I + J + K = R$ but so that it is *not* true that $I + J = R$, nor $I + K = R$, nor $J + K = R$.

#28.244 Give an example of three ideals I, J, K in the ring $R = \mathbf{Z}$ and $a, b, c \in R$ so that the system of three congruences

$$x \equiv a \pmod{I} \quad x \equiv b \pmod{J} \quad x \equiv c \pmod{K}$$

has *no* solution.

29. (*) The Hamiltonian Quaternions

Apart from rings of square matrices of a certain size, there is another very popular example of a *non-commutative* ring, the **Hamiltonian quaternions** \mathbf{H} . In fact, because it turns out that every non-zero element has an multiplicative inverse, this \mathbf{H} is called a *division ring*.

As a set, \mathbf{H} is the set of ‘expressions’

$$a + bi + cj + dk$$

with $a, b, c \in \mathbf{R}$ and where the i, j, k are ‘entities’ satisfying such that

$$i^2 = j^2 = k^2 = -1$$

$$ij = k \quad ji = -k$$

$$jk = i \quad kj = -i$$

$$ki = j \quad ik = -j$$

and also

$$ri = ir \quad rj = jr \quad rk = kr$$

for any $r \in \mathbf{R}$.

Two quaternions $a + bi + cj + dk$ and $a' + b'i + c'j + d'k$ are *equal* if and only if $a = a'$, $b = b'$, $c = c'$, and $d = d'$. In particular, $a + bi + cj + dk = 0$ only if $a = b = c = d = 0$.

(Yes, there are some nagging questions left open by this “definition”: in particular, why are we to be sure that there *exist* such things as these mythical i, j, k ?)

The **quaternion conjugate** $\bar{\alpha}$ is defined in a manner similar to *complex* conjugates, namely, that

$$\bar{\alpha} = \overline{a + bi + cj + dk} = a - bi - cj - dk$$

The **norm** of a quaternion $\alpha = a + bi + cj + dk$ is

$$N\alpha = N(a + bi + cj + dk) = \alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2$$

#29.245 Prove that the quaternion conjugation has the property that, for two quaternions α, β ,

$$\overline{(\alpha\beta)} = \bar{\beta} \cdot \bar{\alpha}$$

#29.246 Check that if a quaternion α is *non-zero*, then then the *norm* $N\alpha = \alpha\bar{\alpha}$ is a *non-zero real number*.

#29.247 Prove that for two quaternions α, β we have the *multiplicativity* property

$$N(\alpha\beta) = N\alpha \cdot N\beta$$

#29.248 Show that \mathbf{H} is a *division ring*, meaning that every non-zero quaternion has a multiplicative inverse.

#29.249 (*) Note that i, j , and k are three different square roots of -1 inside the quaternions. Find *infinitely-many* square roots of -1 inside the quaternions.

30. More about rings

- Cancellation and zero divisors
 - Idempotent and Nilpotent Elements
 - Maximal ideals and fields
 - Prime ideals and integral domains
 - Maximal ideals are prime
 - Euclidean rings
 - Principal ideal domains
-

30.1 Cancellation and zero divisors

The **cancellation property** is the very desirable and reasonable sounding property that, if $c \neq 0$, then $ca = cb$ implies $a = b$. This property is something which *does* hold in rings we are accustomed to, such as the integers, rational numbers, real numbers, and complex numbers. *But it does not hold in all commutative rings*, so we can't take it for granted.

If it does happen that $ca = cb$ with $c \neq 0$ but $a \neq b$, then we rearrange the equation $ca = cb$ to

$$0 = ca - cb = c(a - b)$$

Since $a \neq b$, $a - b \neq 0$. That is, the product $c(a - b)$ is 0, but neither of the factors $c, a - b$ is 0. Generally, if x, y are two elements of some ring so that $x \neq 0$ and $y \neq 0$ but $xy = 0$, then we say that x and y are **zero-divisors**.

To repeat: an element x of a commutative ring R is a **zero-divisor** if x itself is *non-zero* but there is a *non-zero* element y in R so that $xy = 0$. A commutative ring is an **integral domain** if it has *no* zero-divisors.

So the convention pointedly does not consider 0 a zero-divisor. Also, the fact that $r \cdot 0 = 0$ for any r , which looks like it means that *any* r divides 0, does not deter us from giving the definition the way it is!

A commutative ring with no zero-divisors is called an **integral domain**. The fundamental thing here is:

Proposition: A commutative ring R has the *cancellation property* if and only if it is an *integral domain*.

Proof: Suppose that R has the cancellation property. And suppose that $x \cdot y = 0$ for some $x, y \in R$. Since $x \cdot 0 = 0$ for any $x \in R$, we can rewrite this as

$$x \cdot y = x \cdot 0$$

If $x \neq 0$, we can apply the cancellation law, obtaining $y = 0$. Thus, $xy = 0$ implies either $x = 0$ or $y = 0$. This is half of what we want.

Suppose that R is an integral domain. And suppose that $xy = xz$. Then, ‘subtracting’ xz from both sides, we have $xy - xz = 0$, or $x(y - z) = 0$ by un-distributing. If $x \neq 0$, then $y - z$ must be 0. Therefore, for $x \neq 0$ the relation $xy = xz$ implies $y = z$, which is the cancellation property. *Done.*

30.2 Idempotent and Nilpotent Elements

In some rings there are elements which do not behave at all like the “numbers” we are used to. These phenomena can already be seen in the rings \mathbf{Z}/n with n suitable composite numbers.

An element r of a commutative ring R is called **idempotent** if $r^2 = r$.

For example, in any ring there is at least one idempotent element, namely 0. And if there is a *unit* 1 in the ring, then certainly 1 is also an idempotent.

An element r of a commutative ring R is called **nilpotent** if for some integer $n > 1$ we have $r^n = 0$. Thus, usually 0 itself is *not* considered to be nilpotent.

30.3 Maximal ideals and fields

For many purposes we are quite happy when some ‘batch’ of numbers is a *field*, as opposed to something trickier. For example, the quotients \mathbf{Z}/p with p prime are simpler to deal with than \mathbf{Z}/n with ‘highly composite’ numbers n . We only deal with *commutative* rings for this discussion.

Let R be a commutative ring with unit. An ideal M in R is **maximal** if there is no ideal strictly larger than M (containing M) except R itself. Always any ring is an ideal in itself, and to be able to exclude this silly case we say that an ideal other than the ring itself is a **proper ideal**.

Theorem: Let R be a commutative ring with unit and I an ideal. Then R/I is a field if and only if I is a maximal ideal.

Proof: Let $x + I$ be a non-zero element of R/I . Then $x + I \neq I$, so $x \notin I$. Note that the ideal $Rx + I$ is therefore strictly larger than I . Since I was already maximal, it must be that $Rx + I = R$. Therefore, there are $r \in R$ and $i \in I$ so that $rx + i = 1$. Looking at this last equation modulo I , we have $rx \equiv 1 \pmod{I}$. That is, $r + I$ is the multiplicative inverse to $x + I$. Thus, R/I is a field.

On the other hand, suppose that R/I is a field. Let $x \in R$ but $x \notin I$. Then $x + I \neq 0 + I$ in R/I . Therefore, $x + I$ has a multiplicative inverse $r + I$ in R/I . That is,

$$(r + I) \cdot (x + I) = 1 + I$$

From the definition of the multiplication in the quotient, this is $rx + I = 1 + I$, or $1 \in rx + I$, which implies that the ideal $Rx + I$ is R . But $Rx + I$ is the smallest ideal containing I and x . Thus, there cannot be any proper ideal strictly larger than I , so I is maximal. *Done.*

30.4 Prime ideals and integral domains

In this section we only consider *commutative* rings. Just as there was a perfect correspondence between fields R/I and maximal ideals I , there is a perfect correspondence between integral domains and *prime ideals*, defined below.

An ideal I in a ring R is **prime** if $xy \in I$ implies that one or the other (or both) of x, y is in I .

It is at least intuitively clear (although not completely trivial) that for a prime number p in \mathbf{Z} , the ideal $p\mathbf{Z}$ of multiples of p is a *prime ideal*. And, conversely, if an integer $n \neq 0$ is *not* prime, then the ideal $n\mathbf{Z}$ in \mathbf{Z} is *not* prime.

Theorem: Let R be a commutative ring, and I an ideal. Then I is a *prime ideal* if and only if R/I is an *integral domain*.

Proof: Let I be a prime ideal. Suppose that $(x+I) \cdot (y+I) = 0+I$ in R/I , and that $x+I \neq 0+I$. Invoking the definition of multiplication in the quotient, the first hypothesis gives $xy+I = I$, so that $xy \in I$. Yet, by the second hypothesis, $x \notin I$. Therefore, by the prime-ness of I , $y \in I$. That is, $y+I = 0+I$, so $y+I$ is the zero in R/I . This proves that R/I is an integral domain.

On the other hand, suppose that R/I is an integral domain. Let $x, y \in R$ so that $xy \in I$, but $x \notin I$. Then $x+I \neq 0+I$. And $xy \in I$ implies that

$$(x+I) \cdot (y+I) = xy+I = I = 0+I$$

Therefore, since R/I is an integral domain, and since $x+I \neq 0+I$, it must be that $y+I = 0+I$. That is, $y \in I$, as desired. *Done.*

30.5 Maximal ideals are prime

The point of this section is to prove that in any commutative ring with 1 *maximal ideals are prime ideals*. (The converse is not generally true).

Let M be a maximal ideal in a commutative ring R with a unit 1. Let's suppose that $xy \in M$ but that $x \notin M$ and prove that $y \in M$, thereby verifying the defining property of prime ideals.

If it were not the case that $x \in M$, then the set

$$N = M + R \cdot x$$

would be strictly larger than M , since it would contain M and also $x = 0 + 1 \cdot x$. Let's check that this is an ideal. Indeed, with $m, m_1, m_2 \in M$ and with $r, r_o, r_1, r_2 \in R$ we have

$$\begin{aligned} 0_R &= 0 + 0 \cdot x \\ -(m + r \cdot x) &= (-m) + (-r) \cdot x \\ (m_1 + r_1 \cdot x) + (m_2 + r_2 \cdot x) &= (m_1 + m_2) + (r_1 + r_2) \cdot x \\ r(m + r_o \cdot x) &= (rm) + (rr_o) \cdot x \end{aligned}$$

which verifies the requisite properties of an ideal.

But since M was *maximal*, it must be that N is the whole ring R . That is, there are $m \in M$ and $r \in R$ so that

$$1 = m + r \cdot x$$

Then

$$y = y \cdot 1 = y(m + rx) = ym + r(xy) \in yM + rM \subset M + M \subset M$$

since $xy \in M$ and since M is an ideal. This proves that a maximal ideal in a commutative ring with 1 is a prime ideal.

30.6 Euclidean rings

Based on our two most important examples of rings with a *Division Algorithm* and therefore with a *Euclidean Algorithm*, the ordinary integers and polynomials over a field, we abstract the crucial property which makes this work. For the moment, the goal is to prove that *Euclidean rings are principal ideal domains*. This is a stronger property than simply being a unique factorization domain: in the sequel we will prove further that principal ideal domains have the *Unique Factorization* property.

Again, this whole line of argument applies to the ordinary integers as well, so we finally will have *proven* what we perhaps had been taking for granted all along, namely that the ordinary integers really do have unique factorizations into primes. But we might be impatient with the proof for the ordinary integers, since we tend to believe that it is true anyway.

An **absolute value** or **norm** on a commutative ring R is a function usually denoted $|r|$ of elements $r \in R$ having the properties

- *Multiplicativity*: For all $r, s \in R$ we have $|rs| = |r| \cdot |s|$.
- *Triangle inequality*: For all $r, s \in R$ we have $|r + s| \leq |r| + |s|$.
- *Positivity*: If $|r| = 0$ then $r = 0$.

If an absolute value on a ring R has the property that *any non-empty subset S of R has an element of least positive absolute value* (among the collection of absolute values of elements of S), then we say the absolute value is **discrete**.

A commutative ring R is **Euclidean** if there is a *discrete* absolute value on it, denoted $|r|$, so that for any $x \in R$ and for any $0 \neq y \in R$ there are $q, r \in R$ so that

$$x = yq + r \quad \text{with } |r| < |y|$$

The idea is that *we can divide and get a remainder strictly smaller than the divisor*.

The hypothesis that the absolute value be *discrete* in the above sense is critical. Sometimes it is easy to see that this requirement is fulfilled. For example, if $|\cdot|$ is *integer-valued*, as is the case with the usual absolute value on the ordinary integers, then the usual Well-Ordering Principle assures the ‘discreteness’.

The most important examples of Euclidean rings are the ordinary integers \mathbf{Z} and any polynomial ring $k[x]$ where k is a field. The absolute value in \mathbf{Z} is just the usual one, while we have to be a tiny bit creative in the case of polynomials, and define

$$|P(x)| = 2^{\text{degree } P}$$

And $|0| = 0$. Here the number 2 could be replaced by any other number bigger than 1, and the absolute value obtained would work just as well.

- Let R be a Euclidean ring. For an ideal I in R other than $\{0\}$, let i be an element in I so that $|i| \leq |i'|$ for any other $i' \in I$. That is, $|i|$ gives the minimum value of the absolute value on the non-empty subset I of R . Then $I = R \cdot i$. And R is an *integral domain*.

We would paraphrase $I = R \cdot i$ by saying that I is **generated by i** . A commutative ring which is an *integral domain* and in which every ideal is generated by a single element is a **principal ideal domain**. The good properties of principal ideal domains will be considered in the next section. For now, all we want to do is show that *Euclidean rings are principal ideal domains*.

Proof: Again, the *discreteness* hypothesis assures that there is at least one $i \in I$ which takes the minimum positive value among all values of the absolute value function on I . Let j be any other element of I . Using the Euclidean-ness hypothesis, there are $q, r \in R$ with $|r| < |i|$ so that

$$j = qi + r$$

Now

$$r = j - qi \in I + q \cdot I \subset I + I = I$$

since both i and j are in I and I is an ideal, so also the remainder r lies in the ideal I . But i is an element of least *positive* absolute value, so it must be that $|r| = 0$. By the *positivity* of the absolute value, it must be that $r = 0$. Then $j = qi$, so j is a multiple of i as asserted.

Finally, let's check that a Euclidean ring is an *integral domain*, meaning that it has no *zero-divisors*, meaning that if $xy = 0$ then either x or y is 0. Well, if $xy = 0$ then

$$0 = |0| = |xy| = |x| \cdot |y|$$

by the multiplicative property of the norm. Now $|x|$ and $|y|$ are non-negative real numbers, so for their product to be 0 one or the other of $|x|$ and $|y|$ must be 0. And then by the positivity property of the norm it must be that one of x, y themselves is 0, as claimed. *Done.*

A person might notice that we didn't use the triangle inequality at all in this proof. That is indeed so, but in practice anything which is a reasonable candidate for an 'absolute value' in the axiomatic sense suggests itself mostly because it *does* behave like an absolute value in a more down-to-earth sense, which includes a triangle inequality.

And a *proof* that a ring is Euclidean usually makes use of a triangle inequality anyway. But in any case there is little point in trying to evade the triangle inequality.

30.7 Principal ideal domains

Now we prove that certain types of rings have *unique factorization*, from an assumption on the nature of their ideals. This assumption holds for any Euclidean ring (this was proven in the last section), so holds for the ordinary integers and for polynomials over a field.

Repeating the definition: a commutative ring R is a **principal ideal domain** if it is an *integral domain* with a '1' and if every ideal I in R is of the form $I = R \cdot x$ for some element x of R . That is, all elements of I are *multiples* of x . Very often principal ideal domains are referred to as *PID's* for the sake of brevity.

(More generally, in any commutative ring R , an ideal I which is of the form

$$Rx = \{r \cdot x : r \in R\}$$

is called a **principal ideal**. The point is that it is *generated by a single element*. This is a handy property for ideals to have, and it may be a surprise to learn that this property does not hold universally).

While one might think that it is the *unique factorization property* which is the crucial feature of the integers \mathbf{Z} , it turns out that the stronger *principal ideal domain* property is more representative of an accurate intuition for the integers. (Not to mention the even stronger Euclidean property).

We have seen that *Euclidean rings* are *PID's*, so that when we prove (just below) that *PID's* are *UFD's* then we will have shown that *Euclidean rings* are *unique factorization domains*.

Rings which are *not* principal ideal domains are actually *typical* among rings, but a limited experience usually makes it appear otherwise.

- A principal ideal domain is a unique factorization domain.
- An ideal $R \cdot x$ in a principal ideal domain is *prime* if and only if x is either 0 or is a prime element.
- For a prime element p in a principal ideal domain R , the ideal $R \cdot p$ is *maximal*.

Proof: Let $r \neq 0$ be an element of the ring R . We must prove that there *exists* a factorization into primes, and that it is *essentially unique*, in the sense above.

We need to make explicit one more property of principal ideal domains: Suppose that our commutative ring R has the property that, for any ‘ascending chain’ of ideals

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

with containment as indicated, then for some large-enough index n it must be that

$$I_n = I_{n+1} = I_{n+2} = \dots$$

In words, this property is that R has *no infinite ascending chains of ideals*. This property is called the *Noetherian property*, and R is said to be **Noetherian**. (*Emma Noether* was the first person to systematically investigate properties of such rings, in the early part of this century).

The first step in the proof is to show that *principal ideal domains are Noetherian*: The proof is not so long, but is a little ‘abstract’: it is just a little exercise to show that for a collection of ideals of the form

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

the union $I = \bigcup_i I_i$ is also an ideal. Then since R is a principal ideal domain there must be $r_o \in R$ so that $I = R \cdot r_o$. But this element must lie in some one of the ideals I_i , say I_{i_o} , since it lies in the union of them. But then

$$I = R \cdot r_o \subset R \cdot I_{i_o} \subset I_o \subset I$$

so actually $I = I_o$. That is, this ascending chain of ideals is actually *finite*. This proves the Noetherian property of principal ideal domains.

Next, let’s prove that for a Noetherian commutative ring R , if $r \in R$ is non-zero and is a non-unit, then *some* prime divides it. Suppose that *no* prime divides r and reach a contradiction, as follows. The element r itself cannot be prime, or else it certainly has a prime divisor. Thus, it has a *proper divisor* r_1 . The element r_1 likewise cannot be prime, or r has a prime divisor, so r_1 has a proper factor r_2 , and so on. Since r_{i+1} is a *proper* divisor of r_i , it is a little exercise to see that we have $R \cdot r_i \subset R \cdot r_{i+1}$ but $R \cdot r_i \neq R \cdot r_{i+1}$.

Then we get a sequence of ideals

$$R \cdot r \subset R \cdot r_2 \subset R \cdot r_3 \subset \dots$$

in which $R \cdot r_i \neq R \cdot r_{i+1}$. But this would contradict the Noetherian property of R , so *some* prime must divide any non-unit r . Thus we have proven that if r is a non-unit and is non-zero in a principal ideal domain R then *some* prime divides it.

Now we nearly repeat the same argument to show that in a Noetherian integral domain R every non-zero element has a prime factorization: Let $r \in R$ be non-zero. If r is a *unit*, then it is a little exercise to see that *no* primes can divide r , and ‘ r ’ itself is already a prime factorization, simply with no primes occurring.

For a non-zero non-unit r , we know by the previous point that there is *some* prime p_1 dividing r . If r/p_1 is a unit, then

$$r = \left(\frac{r}{p_1}\right) \cdot p_1$$

is the desired prime factorization of r . Suppose r/p_1 is *not* a unit. Then there is a prime p_2 dividing r/p_1 . If r/p_1p_2 is a unit, then we have our prime factorization, and we are done. If it is a non-unit, then a prime p_3 divides it, and so on.

If this process terminates, then we have our desired prime factorization. If not, then it is a little exercise to see that we have a chain of ideals

$$R \cdot r \subset R \cdot \frac{r}{p_1} \subset R \cdot \frac{r}{p_1p_2} \subset \dots$$

And it is a little exercise, using the fact that R is an integral domain, to see that none of the ideals in this chain could be equal to each other. But we would then have an infinite ascending chain of ideals, contradicting the Noetherian property. Thus, we have proven that *in a Noetherian integral domain every non-zero element has a factorization into prime elements.*

Next, let's show that if p is a prime element in a principal ideal domain then the ideal $I = R \cdot p$ 'generated by' p is a *maximal ideal*. If not, then there would be another ideal, call it J , so that $J \neq R$, $J \not\subseteq I$, but $I \subset J$. In particular, there would be $x \in J$ with $x \notin I$. Then

$$J' = R \cdot x + I$$

is an ideal still strictly larger than I but, being contained in J , strictly smaller than the whole ring R . Since R is a principal ideal domain, there is a *generator* g for the ideal J' . That is, $J' = R \cdot g$. That is, p is a multiple of g . Therefore, since p is prime, g is either a unit or is associate to p .

If g is a unit, then

$$J' \supset J' \cdot g^{-1} = R \cdot g \cdot g^{-1} = R \cdot 1 = R$$

contradicting the fact that J' is not the whole ring. Therefore, g must be associate to p , that is, there is a unit u so that $g = up$. But then

$$I \supset I \cdot u = R \cdot pu = R \cdot g = J'$$

contradiction.

Therefore, since assuming $I = R \cdot p$ is non-maximal leads to a contradiction, $R \cdot p$ is maximal.

As a corollary of the previous assertion, we have the essential property of prime elements in a principal ideal domain: Let p be a prime *element* in a principal ideal domain R . Then the *ideal* $R \cdot p$ is a *prime ideal*. That is, For $x, y \in R$, if $p|xy$ then either $p|x$ or $p|y$. Indeed, we just showed that $R \cdot p$ is a maximal ideal, and we had earlier shown that in a commutative ring with unit any *maximal ideal* is a *prime ideal*, so we have the result.

Now we prove *uniqueness* of the prime factorization in a principal ideal domain

Suppose that we have two factorizations

$$up_1 \dots p_m = r = vq_1 \dots q_n$$

in a principal ideal domain R where the p_i and q_j are primes and the u, v are units. The claim is that $m = n$ and that if we renumber the q_j 's then p_i and q_i are *associate*.

Indeed, by the property of primes in a principal ideal domain just proven (and a little induction), p_1 must divide one of the factors v, q_1, \dots, q_n on the right hand side. It can't divide the unit v (as one can readily check!), and since the q_j are primes whichever one of them it divides must actually be *associate* to it. Thus, we can divide both sides by p_1 .

Then the same reasoning shows that p_2 must divide one of the *remaining* q_j 's, so must be associate to it.

It is clear that we can continue in such fashion, using the property of prime elements just proven, to cancel all the factors p_i , although the numbering of the q_j 's certainly might not match, and the q_j 's might also differ by units from the corresponding p_i 's. When all the p_i 's are cancelled, there can't be any q_j 's left, or they would supposedly divide the unit u , which is impossible. (This is an easy little exercise).

Thus, in the slightly qualified sense we've indicated, we have the unique factorization property. *Done.*

#30.250 Find 4 zero-divisors in the ring $\mathbf{Z}/15$.

#30.251 Find 6 nilpotent elements in the ring $\mathbf{Z}/16$.

#30.252 Show by example that the cancellation law does not hold in $\mathbf{Z}/15$.

#30.253 Show that in the ring \mathbf{Z}/n with n a *composite* (that is, not prime) number, the so-called *cancellation law* fails: that is, for such n , find (*non-zero*) elements $a, b, c \in \mathbf{Z}/n$ so that $ca = cb$ but $a \neq b$.

#30.254 Show that there are *no* non-zero nilpotent elements in the ring $\mathbf{Z}/15$.

#30.255 Show that even though the image $f(1_R)$ of the multiplicative identity 1_R of a ring R under a ring homomorphism $f : R \rightarrow S$ may not be 1_S , it is still true that $f(1_R)$ is an *idempotent*.

#30.256 In $\mathbf{Z}/35$, in addition to the idempotents $0, 1$ find two *other* idempotents. (This illustrates the fact that the equation $x^2 = x$ may have some very *unobvious* solutions in rings which behave funnily!)

#30.257 Find $8 = 2 \cdot 2 \cdot 2$ distinct idempotents modulo $5 \cdot 7 \cdot 11$.

#30.258 Find all the nilpotent elements in $\mathbf{Z}/24$.

#30.259 Find all the nilpotent elements in $\mathbf{Z}/125$.

#30.260 Show that for a prime p , the only zero-divisors in \mathbf{Z}/p^n are actually *nilpotents*.

#30.261 Find and describe all the nilpotent elements in \mathbf{Z}/p^n where p is prime and $1 < n$.

#30.262 Show that if n is *not* divisible by p^2 for any prime p , then \mathbf{Z}/n has *no* nilpotent elements.

#30.263 Show that if N is not simply a power of a prime, then there are zero-divisors in \mathbf{Z}/N which are not nilpotent.

#30.264 Show that there *cannot* be a field with just 6 elements in it.

#30.265 Show that there *cannot* be a field with just 10 elements in it.

#30.266 Show that if an integer n is divisible by two distinct primes p, q , then there is no field with n elements.

#30.267 Let R be an *integral domain* with unit 1, and suppose that $Rx = Ry$ for two elements x, y of R . Show that there is a unit $u \in R^\times$ so that $y = ux$.

#30.268 Suppose that in an integral domain R we have $xy = z$ where neither x nor y is a unit. Show that $Rz \subset Rx$ but $Rz \neq Rx$.

31. Tables

- Prime factorizations of numbers under 600
 - Prime numbers under 10,000
 - Primitive roots for primes under 100
-

31.1 Prime factorizations of numbers under 600

2 = 2	3 = 3	4 = 2.2	5 = 5
6 = 2.3	7 = 7	8 = 2.2.2	9 = 3.3
10 = 2.5	11 = 11	12 = 2.2.3	13 = 13
14 = 2.7	15 = 3.5	16 = 2.2.2.2	17 = 17
18 = 2.3.3	19 = 19	20 = 2.2.5	21 = 3.7
22 = 2.11	23 = 23	24 = 2.2.2.3	25 = 5.5
26 = 2.13	27 = 3.3.3	28 = 2.2.7	29 = 29
30 = 2.3.5	31 = 31	32 = 2.2.2.2.2	33 = 3.11
34 = 2.17	35 = 5.7	36 = 2.2.3.3	37 = 37
38 = 2.19	39 = 3.13	40 = 2.2.2.5	41 = 41
42 = 2.3.7	43 = 43	44 = 2.2.11	45 = 3.3.5
46 = 2.23	47 = 47	48 = 2.2.2.2.3	49 = 7.7
50 = 2.5.5	51 = 3.17	52 = 2.2.13	53 = 53
54 = 2.3.3.3	55 = 5.11	56 = 2.2.2.7	57 = 3.19
58 = 2.29	59 = 59	60 = 2.2.3.5	61 = 61
62 = 2.31	63 = 3.3.7	64 = 2.2.2.2.2.2	65 = 5.13
66 = 2.3.11	67 = 67	68 = 2.2.17	69 = 3.23
70 = 2.5.7	71 = 71	72 = 2.2.2.3.3	73 = 73
74 = 2.37	75 = 3.5.5	76 = 2.2.19	77 = 7.11
78 = 2.3.13	79 = 79	80 = 2.2.2.2.5	81 = 3.3.3.3
82 = 2.41	83 = 83	84 = 2.2.3.7	85 = 5.17
86 = 2.43	87 = 3.29	88 = 2.2.2.11	89 = 89
90 = 2.3.3.5	91 = 7.13	92 = 2.2.23	93 = 3.31
94 = 2.47	95 = 5.19	96 = 2.2.2.2.2.3	97 = 97
98 = 2.7.7	99 = 3.3.11	100 = 2.2.5.5	101 = 101
102 = 2.3.17	103 = 103	104 = 2.2.2.13	105 = 3.5.7
106 = 2.53	107 = 107	108 = 2.2.3.3.3	109 = 109
110 = 2.5.11	111 = 3.37	112 = 2.2.2.2.7	113 = 113
114 = 2.3.19	115 = 5.23	116 = 2.2.29	117 = 3.3.13
118 = 2.59	119 = 7.17	120 = 2.2.2.3.5	121 = 11.11
122 = 2.61	123 = 3.41	124 = 2.2.31	125 = 5.5.5
126 = 2.3.3.7	127 = 127	128 = 2.2.2.2.2.2.2	129 = 3.43
130 = 2.5.13	131 = 131	132 = 2.2.3.11	133 = 7.19
134 = 2.67	135 = 3.3.3.5	136 = 2.2.2.17	137 = 137
138 = 2.3.23	139 = 139	140 = 2.2.5.7	141 = 3.47
142 = 2.71	143 = 11.13	144 = 2.2.2.2.3.3	145 = 5.29
146 = 2.73	147 = 3.7.7	148 = 2.2.37	149 = 149
150 = 2.3.5.5	151 = 151	152 = 2.2.2.19	153 = 3.3.17

154 = 2.7.11	155 = 5.31	156 = 2.2.3.13	157 = 157
158 = 2.79	159 = 3.53	160 = 2.2.2.2.5	161 = 7.23
162 = 2.3.3.3.3	163 = 163	164 = 2.2.41	165 = 3.5.11
166 = 2.83	167 = 167	168 = 2.2.2.3.7	169 = 13.13
170 = 2.5.17	171 = 3.3.19	172 = 2.2.43	173 = 173
174 = 2.3.29	175 = 5.5.7	176 = 2.2.2.2.11	177 = 3.59
178 = 2.89	179 = 179	180 = 2.2.3.3.5	181 = 181
182 = 2.7.13	183 = 3.61	184 = 2.2.2.23	185 = 5.37
186 = 2.3.31	187 = 11.17	188 = 2.2.47	189 = 3.3.3.7
190 = 2.5.19	191 = 191	192 = 2.2.2.2.2.3	193 = 193
194 = 2.97	195 = 3.5.13	196 = 2.2.7.7	197 = 197
198 = 2.3.3.11	199 = 199	200 = 2.2.2.5.5	201 = 3.67
202 = 2.101	203 = 7.29	204 = 2.2.3.17	205 = 5.41
206 = 2.103	207 = 3.3.23	208 = 2.2.2.2.13	209 = 11.19
210 = 2.3.5.7	211 = 211	212 = 2.2.53	213 = 3.71
214 = 2.107	215 = 5.43	216 = 2.2.2.3.3.3	217 = 7.31
218 = 2.109	219 = 3.73	220 = 2.2.5.11	221 = 13.17
222 = 2.3.37	223 = 223	224 = 2.2.2.2.2.7	225 = 3.3.5.5
226 = 2.113	227 = 227	228 = 2.2.3.19	229 = 229
230 = 2.5.23	231 = 3.7.11	232 = 2.2.2.29	233 = 233
234 = 2.3.3.13	235 = 5.47	236 = 2.2.59	237 = 3.79
238 = 2.7.17	239 = 239	240 = 2.2.2.2.3.5	241 = 241
242 = 2.11.11	243 = 3.3.3.3.3	244 = 2.2.61	245 = 5.7.7
246 = 2.3.41	247 = 13.19	248 = 2.2.2.31	249 = 3.83
250 = 2.5.5.5	251 = 251	252 = 2.2.3.3.7	253 = 11.23
254 = 2.127	255 = 3.5.17	256 = 2.2.2.2.2.2.2	257 = 257
258 = 2.3.43	259 = 7.37	260 = 2.2.5.13	261 = 3.3.29
262 = 2.131	263 = 263	264 = 2.2.2.3.11	265 = 5.53
266 = 2.7.19	267 = 3.89	268 = 2.2.67	269 = 269
270 = 2.3.3.3.5	271 = 271	272 = 2.2.2.2.17	273 = 3.7.13
274 = 2.137	275 = 5.5.11	276 = 2.2.3.23	277 = 277
278 = 2.139	279 = 3.3.31	280 = 2.2.2.5.7	281 = 281
282 = 2.3.47	283 = 283	284 = 2.2.71	285 = 3.5.19
286 = 2.11.13	287 = 7.41	288 = 2.2.2.2.2.3.3	289 = 17.17
290 = 2.5.29	291 = 3.97	292 = 2.2.73	293 = 293
294 = 2.3.7.7	295 = 5.59	296 = 2.2.2.37	297 = 3.3.3.11
298 = 2.149	299 = 13.23	300 = 2.2.3.5.5	301 = 7.43
302 = 2.151	303 = 3.101	304 = 2.2.2.2.19	305 = 5.61
306 = 2.3.3.17	307 = 307	308 = 2.2.7.11	309 = 3.103
310 = 2.5.31	311 = 311	312 = 2.2.2.3.13	313 = 313
314 = 2.157	315 = 3.3.5.7	316 = 2.2.79	317 = 317
318 = 2.3.53	319 = 11.29	320 = 2.2.2.2.2.2.5	321 = 3.107
322 = 2.7.23	323 = 17.19	324 = 2.2.3.3.3.3	325 = 5.5.13
326 = 2.163	327 = 3.109	328 = 2.2.2.41	329 = 7.47
330 = 2.3.5.11	331 = 331	332 = 2.2.83	333 = 3.3.37
334 = 2.167	335 = 5.67	336 = 2.2.2.2.3.7	337 = 337
338 = 2.13.13	339 = 3.113	340 = 2.2.5.17	341 = 11.31
342 = 2.3.3.19	343 = 7.7.7	344 = 2.2.2.43	345 = 3.5.23
346 = 2.173	347 = 347	348 = 2.2.3.29	349 = 349
350 = 2.5.5.7	351 = 3.3.3.13	352 = 2.2.2.2.2.11	353 = 353
354 = 2.3.59	355 = 5.71	356 = 2.2.89	357 = 3.7.17
358 = 2.179	359 = 359	360 = 2.2.2.3.3.5	361 = 19.19
362 = 2.181	363 = 3.11.11	364 = 2.2.7.13	365 = 5.73

366 = 2.3.61	367 = 367	368 = 2.2.2.2.23	369 = 3.3.41
370 = 2.5.37	371 = 7.53	372 = 2.2.3.31	373 = 373
374 = 2.11.17	375 = 3.5.5.5	376 = 2.2.2.47	377 = 13.29
378 = 2.3.3.3.7	379 = 379	380 = 2.2.5.19	381 = 3.127
382 = 2.191	383 = 383	384 = 2.2.2.2.2.2.2.3	385 = 5.7.11
386 = 2.193	387 = 3.3.43	388 = 2.2.97	389 = 389
390 = 2.3.5.13	391 = 17.23	392 = 2.2.2.7.7	393 = 3.131
394 = 2.197	395 = 5.79	396 = 2.2.3.3.11	397 = 397
398 = 2.199	399 = 3.7.19	400 = 2.2.2.2.5.5	401 = 401
402 = 2.3.67	403 = 13.31	404 = 2.2.101	405 = 3.3.3.3.5
406 = 2.7.29	407 = 11.37	408 = 2.2.2.3.17	409 = 409
410 = 2.5.41	411 = 3.137	412 = 2.2.103	413 = 7.59
414 = 2.3.3.23	415 = 5.83	416 = 2.2.2.2.2.13	417 = 3.139
418 = 2.11.19	419 = 419	420 = 2.2.3.5.7	421 = 421
422 = 2.211	423 = 3.3.47	424 = 2.2.2.53	425 = 5.5.17
426 = 2.3.71	427 = 7.61	428 = 2.2.107	429 = 3.11.13
430 = 2.5.43	431 = 431	432 = 2.2.2.2.3.3.3	433 = 433
434 = 2.7.31	435 = 3.5.29	436 = 2.2.109	437 = 19.23
438 = 2.3.73	439 = 439	440 = 2.2.2.5.11	441 = 3.3.7.7
442 = 2.13.17	443 = 443	444 = 2.2.3.37	445 = 5.89
446 = 2.223	447 = 3.149	448 = 2.2.2.2.2.2.7	449 = 449
450 = 2.3.3.5.5	451 = 11.41	452 = 2.2.113	453 = 3.151
454 = 2.227	455 = 5.7.13	456 = 2.2.2.3.19	457 = 457
458 = 2.229	459 = 3.3.3.17	460 = 2.2.5.23	461 = 461
462 = 2.3.7.11	463 = 463	464 = 2.2.2.2.29	465 = 3.5.31
466 = 2.233	467 = 467	468 = 2.2.3.3.13	469 = 7.67
470 = 2.5.47	471 = 3.157	472 = 2.2.2.59	473 = 11.43
474 = 2.3.79	475 = 5.5.19	476 = 2.2.7.17	477 = 3.3.53
478 = 2.239	479 = 479	480 = 2.2.2.2.2.3.5	481 = 13.37
482 = 2.241	483 = 3.7.23	484 = 2.2.11.11	485 = 5.97
486 = 2.3.3.3.3.3	487 = 487	488 = 2.2.2.61	489 = 3.163
490 = 2.5.7.7	491 = 491	492 = 2.2.3.41	493 = 17.29
494 = 2.13.19	495 = 3.3.5.11	496 = 2.2.2.2.31	497 = 7.71
498 = 2.3.83	499 = 499	500 = 2.2.5.5.5	501 = 3.167
502 = 2.251	503 = 503	504 = 2.2.2.3.3.7	505 = 5.101
506 = 2.11.23	507 = 3.13.13	508 = 2.2.127	509 = 509
510 = 2.3.5.17	511 = 7.73	512 = 2.2.2.2.2.2.2.2.2	513 = 3.3.3.19
514 = 2.257	515 = 5.103	516 = 2.2.3.43	517 = 11.47
518 = 2.7.37	519 = 3.173	520 = 2.2.2.5.13	521 = 521
522 = 2.3.3.29	523 = 523	524 = 2.2.131	525 = 3.5.5.7
526 = 2.263	527 = 17.31	528 = 2.2.2.2.3.11	529 = 23.23
530 = 2.5.53	531 = 3.3.59	532 = 2.2.7.19	533 = 13.41
534 = 2.3.89	535 = 5.107	536 = 2.2.2.67	537 = 3.179
538 = 2.269	539 = 7.7.11	540 = 2.2.3.3.3.5	541 = 541
542 = 2.271	543 = 3.181	544 = 2.2.2.2.2.17	545 = 5.109
546 = 2.3.7.13	547 = 547	548 = 2.2.137	549 = 3.3.61
550 = 2.5.5.11	551 = 19.29	552 = 2.2.2.3.23	553 = 7.79
554 = 2.277	555 = 3.5.37	556 = 2.2.139	557 = 557
558 = 2.3.3.31	559 = 13.43	560 = 2.2.2.2.5.7	561 = 3.11.17
562 = 2.281	563 = 563	564 = 2.2.3.47	565 = 5.113
566 = 2.283	567 = 3.3.3.3.7	568 = 2.2.2.71	569 = 569
570 = 2.3.5.19	571 = 571	572 = 2.2.11.13	573 = 3.191
574 = 2.7.41	575 = 5.5.23	576 = 2.2.2.2.2.2.3.3	577 = 577

578 = 2.17.17	579 = 3.193	580 = 2.2.5.29	581 = 7.83
582 = 2.3.97	583 = 11.53	584 = 2.2.2.73	585 = 3.3.5.13
586 = 2.293	587 = 587	588 = 2.2.3.7.7	589 = 19.31
590 = 2.5.59	591 = 3.197	592 = 2.2.2.2.37	593 = 593
594 = 2.3.3.3.11	595 = 5.7.17	596 = 2.2.149	597 = 3.199
598 = 2.13.23	599 = 599	600 = 2.2.2.3.5.5	601 = 601

31.2 Prime numbers under 10,000

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, 2003, 2011, 2017, 2027, 2029, 2039, 2053, 2063, 2069, 2081, 2083, 2087, 2089, 2099, 2111, 2113, 2129, 2131, 2137, 2141, 2143, 2153, 2161, 2179, 2203, 2207, 2213, 2221, 2237, 2239, 2243, 2251, 2267, 2269, 2273, 2281, 2287, 2293, 2297, 2309, 2311, 2333, 2339, 2341, 2347, 2351, 2357, 2371, 2377, 2381, 2383, 2389, 2393, 2399, 2411, 2417, 2423, 2437, 2441, 2447, 2459, 2467, 2473, 2477, 2503, 2521, 2531, 2539, 2543, 2549, 2551, 2557, 2579, 2591, 2593, 2609, 2617, 2621, 2633, 2647, 2657, 2659, 2663, 2671, 2677, 2683, 2687, 2689, 2693, 2699, 2707, 2711, 2713, 2719, 2729, 2731, 2741, 2749, 2753, 2767, 2777, 2789, 2791, 2797, 2801, 2803, 2819, 2833, 2837, 2843, 2851, 2857, 2861, 2879, 2887, 2897, 2903, 2909, 2917, 2927, 2939, 2953, 2957, 2963, 2969, 2971, 2999, 3001, 3011, 3019, 3023, 3037, 3041, 3049, 3061, 3067, 3079, 3083, 3089, 3109, 3119, 3121, 3137, 3163, 3167, 3169, 3181, 3187, 3191, 3203, 3209, 3217, 3221, 3229, 3251, 3253, 3257, 3259, 3271, 3299, 3301, 3307, 3313, 3319, 3323, 3329, 3331, 3343, 3347, 3359, 3361, 3371, 3373, 3389, 3391, 3407, 3413, 3433, 3449, 3457, 3461, 3463, 3467, 3469, 3491, 3499, 3511, 3517, 3527, 3529, 3533, 3539, 3541, 3547, 3557, 3559, 3571, 3581, 3583, 3593, 3607, 3613, 3617, 3623, 3631, 3637, 3643, 3659, 3671, 3673, 3677, 3691, 3697, 3701, 3709, 3719, 3727, 3733, 3739, 3761, 3767, 3769, 3779, 3793, 3797, 3803, 3821, 3823, 3833, 3847, 3851, 3853, 3863, 3877, 3881, 3889, 3907, 3911, 3917, 3919, 3923, 3929, 3931, 3943, 3947, 3967, 3989, 4001, 4003, 4007, 4013, 4019, 4021, 4027, 4049, 4051, 4057, 4073, 4079, 4091, 4093, 4099, 4111, 4127, 4129, 4133, 4139, 4153, 4157, 4159, 4177, 4201, 4211, 4217, 4219, 4229, 4231, 4241, 4243, 4253, 4259, 4261, 4271, 4273, 4283, 4289, 4297, 4327, 4337, 4339, 4349, 4357, 4363, 4373, 4391, 4397, 4409, 4421, 4423, 4441, 4447, 4451, 4457, 4463, 4481, 4483, 4493, 4507, 4513, 4517, 4519, 4523, 4547, 4549, 4561, 4567, 4583, 4591, 4597, 4603, 4621, 4637, 4639, 4643, 4649, 4651, 4657, 4663, 4673, 4679, 4691, 4703, 4721, 4723, 4729, 4733, 4751, 4759, 4783, 4787, 4789, 4793, 4799, 4801, 4813, 4817, 4831, 4861, 4871, 4877, 4889, 4903, 4909, 4919, 4931, 4933, 4937, 4943, 4951, 4957, 4967, 4969, 4973, 4987, 4993, 4999, 5003, 5009, 5011, 5021, 5023, 5039, 5051, 5059, 5077, 5081, 5087, 5099, 5101, 5107, 5113, 5119, 5147, 5153, 5167, 5171, 5179, 5189, 5197, 5209, 5227, 5231, 5233, 5237, 5261, 5273, 5279, 5281, 5297, 5303, 5309, 5323, 5333, 5347, 5351, 5381, 5387, 5393, 5399, 5407, 5413, 5417, 5419, 5431, 5437, 5441, 5443, 5449, 5471, 5477, 5479, 5483, 5501, 5503, 5507, 5519, 5521, 5527, 5531, 5557, 5563, 5569, 5573, 5581, 5591, 5623, 5639, 5641, 5647, 5651, 5653, 5657, 5659, 5669, 5683, 5689, 5693, 5701, 5711, 5717, 5737, 5741, 5743, 5749, 5779, 5783, 5791, 5801, 5807, 5813, 5821, 5827, 5839, 5843, 5849, 5851, 5857, 5861, 5867, 5869, 5879, 5881, 5897, 5903, 5923, 5927, 5939, 5953, 5981, 5987, 6007, 6011, 6029, 6037, 6043, 6047, 6053, 6067, 6073,

6079, 6089, 6091, 6101, 6113, 6121, 6131, 6133, 6143, 6151, 6163, 6173, 6197, 6199, 6203, 6211, 6217, 6221, 6229, 6247, 6257, 6263, 6269, 6271, 6277, 6287, 6299, 6301, 6311, 6317, 6323, 6329, 6337, 6343, 6353, 6359, 6361, 6367, 6373, 6379, 6389, 6397, 6421, 6427, 6449, 6451, 6469, 6473, 6481, 6491, 6521, 6529, 6547, 6551, 6553, 6563, 6569, 6571, 6577, 6581, 6599, 6607, 6619, 6637, 6653, 6659, 6661, 6673, 6679, 6689, 6691, 6701, 6703, 6709, 6719, 6733, 6737, 6761, 6763, 6779, 6781, 6791, 6793, 6803, 6823, 6827, 6829, 6833, 6841, 6857, 6863, 6869, 6871, 6883, 6899, 6907, 6911, 6917, 6947, 6949, 6959, 6961, 6967, 6971, 6977, 6983, 6991, 6997, 7001, 7013, 7019, 7027, 7039, 7043, 7057, 7069, 7079, 7103, 7109, 7121, 7127, 7129, 7151, 7159, 7177, 7187, 7193, 7207, 7211, 7213, 7219, 7229, 7237, 7243, 7247, 7253, 7283, 7297, 7307, 7309, 7321, 7331, 7333, 7349, 7351, 7369, 7393, 7411, 7417, 7433, 7451, 7457, 7459, 7477, 7481, 7487, 7489, 7499, 7507, 7517, 7523, 7529, 7537, 7541, 7547, 7549, 7559, 7561, 7573, 7577, 7583, 7589, 7591, 7603, 7607, 7621, 7639, 7643, 7649, 7669, 7673, 7681, 7687, 7691, 7699, 7703, 7717, 7723, 7727, 7741, 7753, 7757, 7759, 7789, 7793, 7817, 7823, 7829, 7841, 7853, 7867, 7873, 7877, 7879, 7883, 7901, 7907, 7919, 7927, 7933, 7937, 7949, 7951, 7963, 7993, 8009, 8011, 8017, 8039, 8053, 8059, 8069, 8081, 8087, 8089, 8093, 8101, 8111, 8117, 8123, 8147, 8161, 8167, 8171, 8179, 8191, 8209, 8219, 8221, 8231, 8233, 8237, 8243, 8263, 8269, 8273, 8287, 8291, 8293, 8297, 8311, 8317, 8329, 8353, 8363, 8369, 8377, 8387, 8389, 8419, 8423, 8429, 8431, 8443, 8447, 8461, 8467, 8501, 8513, 8521, 8527, 8537, 8539, 8543, 8563, 8573, 8581, 8597, 8599, 8609, 8623, 8627, 8629, 8641, 8647, 8663, 8669, 8677, 8681, 8689, 8693, 8699, 8707, 8713, 8719, 8731, 8737, 8741, 8747, 8753, 8761, 8779, 8783, 8803, 8807, 8819, 8821, 8831, 8837, 8839, 8849, 8861, 8863, 8867, 8887, 8893, 8923, 8929, 8933, 8941, 8951, 8963, 8969, 8971, 8999, 9001, 9007, 9011, 9013, 9029, 9041, 9043, 9049, 9059, 9067, 9091, 9103, 9109, 9127, 9133, 9137, 9151, 9157, 9161, 9173, 9181, 9187, 9199, 9203, 9209, 9221, 9227, 9239, 9241, 9257, 9277, 9281, 9283, 9293, 9311, 9319, 9323, 9337, 9341, 9343, 9349, 9371, 9377, 9391, 9397, 9403, 9413, 9419, 9421, 9431, 9433, 9437, 9439, 9461, 9463, 9467, 9473, 9479, 9491, 9497, 9511, 9521, 9533, 9539, 9547, 9551, 9587, 9601, 9613, 9619, 9623, 9629, 9631, 9643, 9649, 9661, 9677, 9679, 9689, 9697, 9719, 9721, 9733, 9739, 9743, 9749, 9767, 9769, 9781, 9787, 9791, 9803, 9811, 9817, 9829, 9833, 9839, 9851, 9857, 9859, 9871, 9883, 9887, 9901, 9907, 9923, 9929, 9931, 9941, 9949, 9967, 9973.

31.3 Primitive roots for primes under 100

3 has primitive roots 2.

5 has primitive roots 2, 3.

7 has primitive roots 3, 5.

11 has primitive roots 2, 6, 7, 8.

13 has primitive roots 2, 6, 7, 11.

17 has primitive roots 3, 5, 6, 7, 10, 11, 12, 14.

19 has primitive roots 2, 3, 10, 13, 14, 15.

23 has primitive roots 5, 7, 10, 11, 14, 15, 17, 19, 20, 21.

29 has primitive roots 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27.

31 has primitive roots 3, 11, 12, 13, 17, 21, 22, 24.

37 has primitive roots 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35.

41 has primitive roots 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.

43 has primitive roots 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34.

47 has primitive roots 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45.

53 has primitive roots 2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51.

59 has primitive roots 2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56.

61 has primitive roots 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59.

67 has primitive roots 2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63.

71 has primitive roots 7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69.

73 has primitive roots 5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68.

79 has primitive roots 3, 6, 7, 28, 29, 30, 34, 35, 37, 39, 43, 47, 48, 53, 54, 59, 60, 63, 66, 68, 70, 74, 75, 77.

83 has primitive roots 2, 5, 6, 8, 13, 14, 15, 18, 19, 20, 22, 24, 32, 34, 35, 39, 42, 43, 45, 46, 47, 50, 52, 53, 54, 55, 56, 57, 58, 60, 62, 66, 67, 71, 72, 73, 74, 76, 79, 80.

89 has primitive roots 3, 6, 7, 13, 14, 15, 19, 23, 24, 26, 27, 28, 29, 30, 31, 33, 35, 38, 41, 43, 46, 48, 51, 54, 56, 58, 59, 60, 61, 62, 63, 65, 66, 70, 74, 75, 76, 82, 83, 86.

97 has primitive roots 5, 7, 10, 13, 14, 15, 17, 21, 23, 26, 29, 37, 38, 39, 40, 41, 56, 57, 58, 59, 60, 68, 71, 74, 76, 80, 82, 83, 84, 87, 90, 92