Analytic Number Theory
Winter 2005
Professor C. Stewart

Chris Almost

Contents

Grades: Assignments — 10%, Midterm — 25%, Final — 65%
Midterm: Friday, February 18, 2005; in class
References:

- "An Introduction to the Theory of Numbers" by Hardy and Wright (Cambridge Press)
- "Introduction to Analytic Number Theory" by Apostel (Springer-Verlag)

1 Introduction

1.1 Definition. A *prime number* is a positive integer greater than 1 such that the only positive factors of it are 1 and itself. Let $\pi(x)$ denote the number of primes less than or equal to x.

Basic Question: How are the primes distributed amoung the integers? How does $\pi(x)$ grow with x?

Let p_n denote the n^{th} prime. Is there a polynomial $f \in \mathbb{Z}[x]$ such that $f(n) = p_n$? Clearly no, as if q is prime and $q|f(n)$ then $q|f(n+kq)$ for all $k \in \mathbb{N}$. This observation shows further that any polynomial that takes only prime values on the integers must be constant. There are examples of polynomials whose initial values are surprisingly often prime. For example, Euler noticed that n^2+n+41 is prime for $n = 0, \dots, 39$, and by translation, $(n-40)^2 + (n-40) + 41$ is prime for $n = 0, \dots, 79$. This is related to the fact that $\mathbb{Q}(\sqrt{-163})$ has class number 1. In the 70's Matijasevic proved Hilbert's 10^{th} problem, and in the process was able to prove that there is a polynomial $f \in \mathbb{Z}[a, b, c, \dots, z]$ such that the positive values in $f(\mathbb{N}^{26})$ is exactly the set of primes. In 1977 he showed that 10 variables suffices.

Can we find a non-constant polynomial $f \in \mathbb{Z}[x]$ such that $f(n)$ is prime infinitely often? Clearly yes, $f(x) = x + k$ works for any $k \in \mathbb{Z}$. Dirichlet showed that for coprime $k, \ell \in \mathbb{N}$ there are infinitely many primes of the form $kn + \ell$. Is $x^2 + 1$ prime infinitely often? Almost surely yes, but the best result known to date is that $n^2 + 1$ is a product of two primes for infinitely many n. There is no polynomial of degree greater than one in one variable known to take prime values infinitely often. If instead we consider polynomials of two variables we can go further. Friedlander and Iwaniec (1998) proved that there are infinitely many primes of the form $n^2 + m^4$. In (2001) Heath Brown proved there are infinitely many primes of the form $n^3 + 2m^3$.

Let the Möbius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$ be defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is squarefree and } k \text{ is the number of distinct prime factors of } n \\ 0 & \text{otherwise} \end{cases}$$

In 1971, Gandhi proved that if $Q_n := p_1 \dots p_n$, where p_i is the i^{th} prime, then p_{n+1} is the unique integer which satisfies the inequality

$$1 < 2^{p_{n+1}} \left(-\frac{1}{2} + \sum_{d|Q_n} \frac{\mu(d)}{2^d - 1} \right) < 2$$

(S. Golmab, American Mathematical Monthly, 1974, p. 752-754)

Recall Wilson's Theorem, that an integer $n > 1$ is prime if and only if $n|(n-1)! + 1$. Thus, for $x > 1$,

$$\pi(x) = \sum_{2 \le j \le x} \left(\left[\frac{(j-1)! + 1}{j} \right] - \left[\frac{(j-1)!}{j} \right] \right)$$

where $[\cdot]$ is the greatest integer function. This estimate is not particularily useful, as $n!$ is extremely large compared to n.

1.2 Theorem (Euclid). *There are infinitely many primes.*

Proof: Assume not. If $p_1, \dots, p_n$ are all of the primes, then $p_1 \dots p_n + 1$ has no prime factors. This is a contradiction. □

Notice that we can extract a bound for $\pi(x)$ from Euclid's proof. By an easy induction we can prove that $p_n \le 2^{2^n}$ for all n. Indeed, $p_1 = 2 \le 2^{2^1}$, and $p_{n+1} \le p_1 \dots p_n \le 2^{2+\dots+2^n} + 1 = 2^{2^{n+1}-2} + 1 \le 2^{2^{n+1}}$. Therefore for $x > 1$, $\pi(x)$ satisfies $2^{2^{\pi(x)}} \le x < 2^{2^{\pi(x)+1}}$. Taking logarithms, $\log_2(\log_2 x) - 1 < \pi(x)$.

2 Elementary Approximations of $\pi(x)$

Fermat numbers are integers of the form $2^{2^n}+1$, $n \ge 0$. He observed that $F_n := 2^{2^n}+1$ is prime for $n = 0,1,2,3,4$. He conjectured that this would always be the case. Almost certainly he was absolutely wrong. 641 divides F_5, and F_n is known to be composite for $n = 5, 6, \dots, 32$.

2.1 Theorem (Pólya). *For any integers n, m with $1 \le n < m$, $\gcd(F_n, F_m) = 1$.*

Proof: Let us put $m = n + k$. Observe that the polynomial $x^{2^k} - 1$ is divisible by $x + 1$ in $\mathbb{Z}[x]$. In particular,

$$\frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \dots - 1$$

If we take $x = 2^{2^n}$ then we get $F_n | F_m - 2$. The result follows since no Fermat number is even. □

As an immediate consequence of this, $p_n \le 2^{2^n} + 1$. Also note that for $x > 1$,

$$2^{\pi(x)} \ge \prod_{p \le x} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \ge \sum_{n \le x} \frac{1}{n} \ge \int_1^x \frac{du}{u} = \log x$$

Thus $\pi(x) \ge \frac{\log\log x}{\log 2}$.

2.2 Theorem. *Let $x \in \mathbb{Z}$, $x \ge 2$. Then*

$$\pi(x) \ge \frac{1}{2\log 2} \log x \quad \textit{and} \quad p_n \le 4^n$$

Proof: Let $p_1, \dots, p_k$ be the primes less than or equal to x. For any $n \in \mathbb{Z}$ with $1 \le n \le x$ we may write $n = n_1^2 m$ where $n_1 \in \mathbb{N}$ and m is square-free. Then $m = p_1^{\varepsilon_1} \dots p_k^{\varepsilon_k}$ where $\varepsilon_i \in \{0, 1\}$. Thus there are at most 2^k possible choices for m. Since $1 \le n \le x$, we see that there are at most $\sqrt{x}$ choices for n_1. Thus there are at most $2^k\sqrt{x}$ numbers between 1 and x, which implies that $x \le 2^k\sqrt{x}$ and hence $\sqrt{x} \le 2^k$. Whence $\frac{1}{2\log 2} \log x \le k = \pi(x)$. Taking $x = p_n$ gives $k = n$ and $\sqrt{p_n} \le 2^n$, so $p_n \le 4^n$. □

Let p be a prime and $n \in \mathbb{N}$. What is the power of p that divides $n!$? Clearly it is

$$\sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] = \sum_{i=1}^{[\log_p n]} \left[\frac{n}{p^i}\right]$$

2.3 Theorem. *Let $x \geq 2$. Then*

$$\frac{3\log 2}{8}\frac{x}{\log x} < \pi(x) < 6\log 2\frac{x}{\log x}$$

PROOF: For each prime p, let r_p denote the unique integer for which $p^{r_p} \leq 2n < p^{r_p+1}$. Then the power of p dividing $\binom{2n}{n}$ is

$$\sum_{k=1}^{r_p}\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]$$

which is less that or equal to r_p, since each term in the sum is either 0 or 1. Therefore $\binom{2n}{n}$ divides $\prod_{p\leq 2n} p^{r_p}$. Hence $2^n \leq \binom{2n}{n} \leq (2n)^{\pi(2n)}$, so $n\log 2 \leq \pi(2n)\log(2n)$ and we get that

$$\frac{\log 2}{2}\frac{2n}{\log(2n)} \leq \pi(2n)$$

Given x, choose n so that $2n \leq x < 2n+2$, so $\pi(x) \geq \frac{\log 2}{2}\frac{2n}{\log(2n)}$. Suppose $x > 6$. Then $2n > \frac{3}{4}x$ and, since $\frac{y}{\log y}$ is increasing for $y > 6$, we have $\frac{3\log 2}{8}\frac{x}{\log x} < \pi(x)$. The result follows for $2 \leq x \leq 6$ as may be checked.

For the upper bound, observe that $\prod_{n<p\leq 2n} p$ divides $\binom{2n}{n}$. Hence $n^{\pi(2n)-\pi(n)} \leq \prod_{n<p\leq 2n} p \leq \binom{2n}{n} \leq 4^n$, so $\pi(2n)\log n - \pi(n)\log n \leq 2n\log 2$. Thus

$$\pi(2n)\log n - \pi(n)\log\frac{n}{2} \leq (2\log 2)n + \pi(n)\log 2 \leq (3\log 2)n$$

If $n = 2^k, 2^{k-1}, \ldots 4$ then we get a telescoping collection of inequalities

$$\begin{gathered}\pi(2^{k+1})\log 2^k - \pi(2^k)\log 2^{k-1} \leq (3\log 2)2^k \\ \pi(2^k)\log 2^{k-1} - \pi(2^{k-1})\log 2^{k-2} \leq (3\log 2)2^{k-1} \\ \vdots \\ \pi(8)\log 4 - \pi(4)\log 2 \leq (3\log 2)4\end{gathered}$$

Adding gives $\pi(2^{k+1})\log 2^k < (3\log 2)2^{k+1}$, hence $\pi(2^{k+1}) < 6\log 2\left(\frac{2^k}{\log 2^k}\right)$. Therefore given x we choose k so that $2^k \leq x < 2^{k+1}$. Whence

$$\pi(x) \leq \pi(2^{k+1}) < 6\log 2\left(\frac{2^k}{\log 2^k}\right) < 6\log 2\left(\frac{x}{\log x}\right)$$

for $x > 4$. Checking the result for $2 \leq x \leq 4$ completes the proof. □

3 Bertrand's Postulate

In 1845 Bertrand found that for $1 \leq n \leq 10^6$ there was always a prime between n and $2n$. He postulated that this always occurs. In 1850 Chebyshev proved it true for all $n \geq 1$. Note that this is not trivial, in that it doesn't occur for free just because $\pi(x) \approx \frac{x}{\log x}$. Take S to be the set containing $[2^{3^n}, 2^{3^{n+1}}]$ for each n. Then S does not have this property, and it is quite a bit more dense than the set of primes.

3.1 Theorem. *For all $n \in \mathbb{N}$,*

$$\prod_{p \le n} p < 4^n$$

PROOF: By induction on n. Clearly the theorem holds for $n = 1, 2$. Suppose that the theorem holds for $k = 1, \dots, n-1$, with $n \ge 3$. Observe that we may restrict our attention to odd n, since if n is even then it is not prime and $\prod_{p \le n} p^n = \prod_{p \le n-1} p^n$. Take $n = 2m+1$ where $m \in \mathbb{N}$. Note that every prime p with $m+2 \le p \le 2m+1$ divides $\binom{2m+1}{m}$, so $\prod_{m+2 \le p \le 2m+1} p$ divides $\binom{2m+1}{m}$. It follows that

$$\prod_{p \le 2m+1} p \le \binom{2m+1}{m} \prod_{p \le m+1} p \le \binom{2m+1}{m} 4^{m+1} \le 4^m 4^{m+1} = 4^{2m+1}$$

since $\binom{2m+1}{m} = \binom{2m+1}{m+1}$ and they both occur in the binomial expansion of $(1+1)^{2m+1}$. □

Notation. If p is a prime and n is an integer and $p^a \mid n$ but $p^{a+1} \nmid n$ then we abbreviate this by $p^a \| n$.

3.2 Lemma. *If $n \ge 3$ and p is a prime with $\frac{2}{3}n < p \le n$ then $p \nmid \binom{2n}{n}$.*

PROOF: Since $n \ge 3$ we see that p is odd. The only multiples of p with $p \le 2n$ are p and $2p$. Thus $p \| n!$ and $p^2 \| (2n)!$. Hence $p \nmid \binom{2n}{n}$. □

3.3 Theorem (Bertrand's Postulate). *For any $n \in \mathbb{N}$ there is a prime p with $n < p \le 2n$.*

PROOF: The result holds for $n = 1, 2, 3$. We argue by contradiction. Suppose that result is false for some integer $n \ge 4$. By Lemma 3.2 there is no prime larger than $\frac{2}{3}n$ which divides $\binom{2n}{n}$. Let p be a prime with $p \le \frac{2}{3}n$ and let a_p be the number such that $p^{a_p} \| \binom{2n}{n}$. As in the proof of Theorem 2.3 we see that $a_p \le r_p$, where r_p is that integer for which $p^{r_p} \le 2n < p^{r_p+1}$. Thus

$$\binom{2n}{n} \le \prod_{p \le \frac{2}{3}n} p^{a_p} \quad \text{and so} \quad \binom{2n}{n} \le (2n)^t \prod_{p \le \frac{2}{3}n} p$$

where t is number of primes $p \le \frac{2}{3}n$ for which $a_p \ge 2$. Since $p^{a_p} \le 2n$ we see that $t \le \sqrt{2n}$. Therefore

$$\binom{2n}{n} \le (2n)^{\sqrt{2n}} \prod_{p \le \frac{2}{3}n} p \le (2n)^{\sqrt{2n}} 4^{\frac{2}{3}n} \qquad \text{by Theorem 3.1}$$

But $\binom{2n}{n} > \frac{4^n}{2n+1}$. Thus $\frac{4^n}{2n+1} < (2n)^{\sqrt{2n}} 4^{\frac{2}{3}n}$, so

$$4^{\frac{n}{3}} < (2n)^{\sqrt{2n}}(2n+1) < (2n)^{\sqrt{2n}+2}$$

We can now check that the result holds when $4 \le n \le 16$, so assume that $n > 16$. Taking logarithms,

$$\frac{\log 4}{3} n < (\sqrt{2n}+2)\log 2n < 2\sqrt{n}\log 2n < 2\sqrt{n}\log n^{\frac{5}{4}} < \frac{5}{2}\sqrt{n}\log n$$

Hence $\frac{\sqrt{n}}{\log n} < \frac{15}{2\log 4}$, and $\frac{\sqrt{n}}{\log n}$ is increasing for $n > e^2$. Furthermore, $\frac{\sqrt{1600}}{\log 1600} = 5.421\ldots > \frac{15}{2\log 4}$, so $n < 1600$. But $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 557, 1109, 2207$ are all prime and so the result follows. □

The obvious question to ask now is whether we can do better. Baker and Harman proved that there is a positive number C such that for $x > C$ there is a prime in the interval $[x, x + x^{0.535}]$. This is the best result known so far. Assuming the Riemann Hypothesis we can replace 0.535 with $\frac{1}{2} + \varepsilon$. In 1930, Cramer conjectured that

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^2} = 1$$

He arrived at this conjecture by probabilistic reasoning. We expect that $p_{n+1} - p_n = 2$ for infinitely many n. This is known as the twin primes conjecture. The best result known on small gaps is due to Maier in 1985. He proved that $p_{n+1} - p_n < (0.248\ldots)\log p_n$ for infinitely many positive integers n.

Can one prove that there are large gaps infinitely often? In 1935, Erdös proved that there is a positive number c such that, for infinitely many positive integers n, $p_{n+1} - p_n > c \log n \frac{\log\log p_n}{(\log\log\log p_n)^2}$. In 1938, Rankin added a factor of $\log\log\log\log p_n$. Erdös offered \$10,000 USD for any proof which showed one could replace the constant c by any function tending to infinity with n.

4 Asymtotic Analysis

Notation. Let $f, g : \mathbb{N} \to \mathbb{R}$ and suppose that $g > 0$. We write $f = O(g)$ whenever there are $c_1, c_2 > 0$ such that if $x > c_1$ then $|f(x)| < c_2 g(x)$. We write $f = o(g)$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$ We write $f \sim g$, pronouced "f is asymtotic to g" if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$

Recall that one of the aims of this course is to prove the Prime Number Theorem, which states that

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

or, equivalently $\pi(x) = \frac{x}{\log x} + o(\frac{x}{\log x})$. Let $\varepsilon > 0$. Notice that

$$\frac{(1+\varepsilon)x}{\log x + \log(1+\varepsilon)} = \frac{(1+\varepsilon)x}{\log x \left(1 + \frac{\log(1+\varepsilon)}{\log x}\right)} = (1+\varepsilon)\frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right) = (1+\varepsilon)\frac{x}{\log x} + o\left(\frac{x}{\log x}\right)$$

since $1 - y + y^2 > \frac{1}{1+y} > 1 - y$ for all $|y| < 1$. Then

$$\pi((1+\varepsilon)x) - \pi(x) = \frac{(1+\varepsilon)x}{\log(1+\varepsilon)x} - \frac{x}{\log x} + o\left(\frac{x}{\log x}\right) = \frac{\varepsilon x}{\log x} + o\left(\frac{x}{\log x}\right)$$

This says that the number of primes between x and $(1+\varepsilon)x$ is about $\frac{\varepsilon x}{\log x}$, which is a much stronger result than Bertrand's Postulate. Taking $\varepsilon = 1$ we have $\pi(2x) - \pi(x) = \frac{x}{\log x} + o(\frac{x}{\log x})$. This seems to suggest that π is linear, but this is not the case.

For any integer n, let

$$\Lambda(n) := \begin{cases} \log p & \text{if } n \text{ is a positive power of } p \\ 0 & \text{otherwise} \end{cases}$$

We define

$$\theta(x) := \sum_{p \le x} \log p$$

and

$$\Psi(x) := \sum_{p^m \le x} \log p = \sum_{n \le x} \Lambda(x)$$

Observe that $\Psi(x) = \sum_{p\le x}\left[\frac{\log x}{\log p}\right]\log p$. Notice that $\theta(x) = \sum_{p\le x}\log p \le x\log x$ and thus

$$\begin{aligned}\Psi(x) &= \theta(x) + \theta(\sqrt{x}) + \theta(\sqrt[3]{x}) + \cdots + \theta(\sqrt[k]{x}) && \text{where } k = \left[\frac{\log x}{\log 2}\right]\\ &\le \theta(x) + \sqrt{x}\log x + \cdots + \sqrt[k]{x}\log x\\ &\le \theta(x) + (\sqrt{x}\log x)\frac{\log x}{\log 2}\\ &= \theta(x) + O(\sqrt{x}(\log x)^2)\end{aligned}$$

By Theorem 2.3, there is a $c_1 > 0$ such that $\theta(x) < c_1 x$ for $x \ge 2$, since $\theta(x) = \sum_{p\le x}\log x \le \pi(x)\log x$. Therefore there is a $c_2 > 0$ such that $\Psi(x) < c_2 x$ for $x \ge 2$. Furthermore, the proof of Theorem 2.3 shows

$$n\log 2 = \log 2^n \le \log\binom{2n}{n} \le \sum_{p\le 2n}\left[\frac{\log 2n}{\log p}\right]\log p = \Psi(2n)$$

for $n \in \mathbb{N}$. Therefore there is a $c_3 > 0$ such that $\Psi(x) > c_3 x$ for $x \ge 2$. As a consequence of this there is a $c_4 > 0$ such that $\theta(x) > c_4 x$ for $x \ge 2$.

4.1 Theorem.

$$\pi(x)\log x \sim \theta(x) \sim \psi(x)$$

Proof: $\theta(x) \sim \psi(x)$ since $\theta(x) \ge c_4 x$ for $x \ge 2$ and $\Psi(x) = \theta(x) + O(\sqrt{x}(\log x)^2)$. It remains to show that $\pi(x)\log x \sim \theta(x)$. Clearly $\pi(x) \ge \frac{\theta(x)}{\log x}$. Let $1 > \delta > 0$. Then

$$\begin{aligned}\theta(x) &\ge \sum_{x^{1-\delta}<p\le x}\log p\\ &\ge \sum_{x^{1-\delta}<p\le x}(1-\delta)\log x\\ &\ge (\pi(x) - \pi(x^{1-\delta}))(1-\delta)\log x\\ &\ge (\pi(x) - x^{1-\delta})(1-\delta)\log x\\ \theta(x) + x^{1-\delta}(1-\delta)\log x &\ge (1-\delta)\pi(x)\log x\end{aligned}$$

Therefore

$$1 \le \frac{\pi(x)\log x}{\theta(x)} \le \frac{1}{1-\delta}\left(1 + \frac{(1-\delta)x^{1-\delta}\log x}{\theta(x)}\right) \le \frac{1}{1-\delta} + \frac{x^{1-\delta}\log x}{\theta(x)}$$

Since $\theta(x) > c_4 x$ for $x \ge 2$ we see that

$$1 \le \frac{\pi(x)\log x}{\theta(x)} \le \frac{1}{1-\delta} + \frac{\log x}{c_4 x^{\delta}}$$

Given $\varepsilon > 0$, choose $\delta > 0$ so that $\frac{1}{1-\delta} < 1 + \frac{\varepsilon}{2}$ and choose $x_0(\varepsilon,\delta)$ so that for $x > x_0(\varepsilon,\delta)$, $\frac{\log x}{c_4 x} < \frac{\varepsilon}{2}$. Then

$$1 \le \frac{\pi(x)\log x}{\theta(x)} \le 1 + \varepsilon$$

and the result follows. □

4.2 Lemma (Abel's summation Formula). *Let $(a_n)_{n=1}^{\infty}$ be a sequence of complex numbers and let f be a continuously differentiable function from $\{x \in \mathbb{R} \mid x \geq 1\}$ to $\mathbb{C}$. For each $x \in \mathbb{R}$ we define $A(x) = \sum_{n \leq x} a_n$. Then*

$$\sum_{n \leq x} a_n f(n) = A(x)f(x) - \int_1^x A(u)f'(u)du$$

PROOF: Put $N = [x]$. Then

$$\begin{aligned}\sum_{n \leq x} a_n f(n) &= \sum_{i=1}^{N} a_i f(i)\\ &= A(1)f(1) + \sum_{i=2}^{N}(A(i) - A(i-1))f(i)\\ &= \sum_{i=1}^{N-1} A(i)(f(i) - f(i+1)) + A(N)f(N)\\ &= A(N)f(N) - \sum_{i=1}^{N-1}\int_i^{i+1} A(u)f'(u)du\end{aligned}$$

Therefore

$$\sum_{n \leq x} a_n f(n) = A(N)f(N) - \int_1^N A(u)f'(u)du$$

but $\int_N^x A(u)f'(u)du = A(x)f(x) - A(N)f(N)$, and the result follows. □

4.3 Definition. *Euler's constant* γ is defined by

$$\gamma := 1 - \int_1^{\infty} \frac{u - [u]}{u^2} du \approx 0.5772\ldots$$

Open Question: Is γ irrational?

4.4 Theorem.

$$\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$$

PROOF: By Lemma 4.2. We take $f(x) = \frac{1}{x}$ and $a_n = 1$ for each n. Then $A(x) = [x]$, and thus

$$\begin{aligned}\sum_{n \leq x} \frac{1}{n} &= [x]\frac{1}{x} + \int_1^x \frac{[u]}{u^2} du\\ &= \frac{x - (x - [x])}{x} + \int_1^x \frac{u - (u - [u])}{u^2} du\\ &= 1 + O\left(\frac{1}{x}\right) + \int_1^x \frac{du}{u} - \int_1^x \frac{u - [u]}{u^2} du\\ &= \log x + \gamma + \int_x^{\infty} \frac{u - [u]}{u^2} du + O\left(\frac{1}{x}\right)\\ &= \log x + \gamma + O\left(\frac{1}{x}\right)\end{aligned}$$

□

4.5 Theorem.

$$\sum_{n\le x}\frac{\Lambda(n)}{n}=\log x+O(1)$$

PROOF: Take $a_n=1$ and $f(x)=\log x$ in Lemma 4.2. Then

$$\begin{aligned}\sum_{n\le x}\log n &= [x]\log x-\int_1^x\frac{[u]}{u}du\\ &=(x-(x-[x]))\log x-\int_1^x\frac{u-([u]-u)}{u}du\\ &=x\log x+O(\log x)-(x-1)+\int_1^x\frac{[u]-u}{u}du\\ &=x\log x-x+O(\log x)+O\left(\int_1^x\frac{1}{u}du\right)\\ &=x\log x-x+O(\log x)\end{aligned}$$

Note that $\log[x]!=\sum_{n\le x}\log n$, so this is a weak form of Stirling's formula. But

$$\begin{aligned}\log[x]! &= \sum_{p\le x}\left(\left[\frac{x}{p}\right]+\left[\frac{x}{p^2}\right]+\cdots\right)\log p\\ &=\sum_{p\le x}\left(\sum_{m=1}^{\left[\frac{\log x}{\log p}\right]}\left[\frac{x}{p^m}\right]\right)\log p\\ &=\sum_{p\le x}\left[\frac{x}{n}\right]\Lambda(n)\\ &=\sum_{n\le x}\left(\frac{x}{n}-\left(\frac{x}{n}-\left[\frac{x}{n}\right]\right)\right)\Lambda(n)\\ &=x\sum_{n\le x}x\frac{\Lambda(n)}{n}-O\left(\Psi(x)\right)\\ &=x\sum_{n\le x}x\frac{\Lambda(n)}{n}-O\left(x\right)\end{aligned}$$

Thus from the first equation,

$$\begin{aligned}x\log x-x+O(\log x)&=x\sum_{n\le x}\frac{\Lambda(n)}{n}-O(x)\\ x\log x+O(x)&=x\sum_{n\le x}\frac{\Lambda(n)}{n}\\ \log x+O(1)&=\sum_{n\le x}\frac{\Lambda(n)}{n}\end{aligned}$$

□

4.6 Theorem.

$$\sum_{p\le x}\frac{\log p}{p}=\log x+O(1)$$

PROOF:

$$\sum_{n\le x}\frac{\Lambda(n)}{n}-\sum_{p\le x}\frac{\log p}{p}=\sum_{\substack{p^m\le x\\ m\ge 2}}\frac{\log p}{p^m}$$

Thus by Theorem 4.5 it suffices to show that the right hand side is $O(1)$. But $\frac{1}{p^2}+\frac{1}{p^3}+\cdots=\frac{1}{p(p-1)}$ and so

$$\sum_{\substack{p^m\le x\\ m\ge 2}}\frac{\log p}{p^m}\le\sum_{2\le n\le x}\frac{\log n}{n(n-1)}\le\sum_{n=2}^{\infty}\frac{\log n}{n(n-1)}<\infty$$

and the result follows. □

4.7 Theorem. *There is a number B_1 such that*

$$\sum_{p\le x}\frac{1}{p}=\log\log x+B_1+o(1)$$

PROOF: Take

$$a_n=\begin{cases}\frac{\log p}{p} & \text{if } n=p\\ 0 & \text{otherwise}\end{cases}$$

and $f(x)=\frac{1}{\log x}$. By Lemma 4.2

$$\begin{aligned}\sum_{p\le x}\frac{1}{p}&=\left(\sum_{p\le x}\frac{\log p}{p}\right)\frac{1}{\log x}+\int_1^x\left(\sum_{p\le u}\frac{\log p}{p}\right)\frac{1}{u(\log u)^2}du\\
&=1+O\left(\frac{1}{\log x}\right)+\int_2^x\frac{A(u)}{u(\log u)^2}du && \text{by Theorem 4.6}\\
&=1+O\left(\frac{1}{\log x}\right)+\int_2^x\frac{\log u+\tau(u)}{u(\log u)^2}du && \text{where } \tau(u)=O(1)\text{, by Lemma 4.2}\\
&=1+O\left(\frac{1}{\log x}\right)+\int_2^x\frac{1}{u\log u}du+\int_2^x\frac{\tau(u)}{u(\log u)^2}du\\
&=\log\log x+1-\log\log 2+O\left(\frac{1}{\log x}\right)+\int_2^x\frac{\tau(u)}{u(\log u)^2}du\\
&=\log\log x+B_1-\int_x^\infty\frac{\tau(u)}{u(\log u)^2}du+O\left(\frac{1}{\log x}\right) && B_1:=1-\log\log 2+\int_2^\infty\frac{\tau(u)}{u(\log u)^2}du\\
&=\log\log x+B_1+o(1)\end{aligned}$$

□

B_1 can be calculated to about $0.261447\ldots$ It can be shown that $B_1=\gamma+\sum_p\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)$.

5 Riemann's Zeta Function

The Riemann zeta function, $\zeta(s)$ is a function of a complex variable s. It is defined for $\Re(s) > 1$ by

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

Since $\sum_{n=1}^{\infty} \frac{1}{n^s}$ is uniformly convergent on compact subsets of $\{z \in \mathbb{C} \mid \Re(z) > 1\}$ we deduce that $\zeta(s)$ is an analytic function on $\Re(s) > 1$. We also note that $\zeta(s)$ may be represented by an Euler product in the same region. Observe that

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

by the Fundemental Theorem of Arithmetic. Since $\zeta(s)$ is represented by a convergent infinite product for $\Re(s) > 1$, we conclude that $\zeta(s) \neq 0$ for $\Re(s) > 1$.

Notation. For the remainder of this section, s denotes a complex number and we put $s = \sigma + it$, with $\sigma, t \in \mathbb{R}$.

5.1 Theorem. *$\zeta(s)$ can be analytically continued to $\Re(s) > 0$, with the exception of a simple pole at $s = 1$ with residue 1.*

Proof: Let $s \in \mathbb{C}$ with $\Re(s) > 1$. We apply Abel summation with $a_n = 1$ and $f(x) = \frac{1}{x^s}$. Then

$$\sum_{n \le y} \frac{1}{n^s} = \frac{[y]}{y^s} + s \int_1^y \frac{[u]}{u^{s+1}} du$$

Letting $y \to \infty$ we find that

$$\begin{aligned} \zeta(s) &= s \int_1^{\infty} \frac{[u]}{u^{s+1}} du \\ &= s \int_1^{\infty} \frac{u - (u - [u])}{u^{s+1}} du \\ &= s \int_1^{\infty} \frac{1}{u^s} du - s \int_1^{\infty} \frac{u - [u]}{u^{s+1}} du \\ &= \frac{s}{s-1} - s \int_1^{\infty} \frac{u - [u]}{u^{s+1}} du \end{aligned}$$

The first term in the sum is analytic on $\mathbb{C}$, except at the point $s = 1$ where it has a simple pole of residue 1. The integral in the second term is uniformly convergent on compact subsets of $\Re(s) > 0$. Furthermore, it represents an analytic function on $\Re(s) > 0$. Thus $\zeta(s)$ may be analytically continued to $\Re(s) > 0$, with the exception of the simple pole at $s = 1$. □

$\zeta(s)$ can be analytically continued to all of $\mathbb{C}$, except for $s = 1$. There is a functional eqution which relates the behavior of $\zeta(s)$ with the behavior of $\zeta(1-s)$. The region $\{s \in \mathbb{C} \mid 0 \le \Re(s) \le 1\}$ is known as the critical strip, and information on the zeroes of $\zeta(s)$ in the critical strip can be translated into information on the distribution of prime numbers. We shall deduce the prime number theorem from the fact that $\zeta(s)$ is not zero for $\Re(s) = 1$.

5.2 Conjecture (Riemann Hypothesis). *All of the zeroes of $\zeta(s)$ in the critical strip satisfy $\Re(s) = \frac{1}{2}$.*

5.3 Theorem. *$\zeta(s)$ is non-zero for $\Re(s) \geq 1$.*

PROOF: We have already seen from the Euler product representation of $\zeta(s)$ that $\zeta(s) \neq 0$ for $\Re(s) > 1$. Thus we may restrict our attention to $\Re(s) = 1$. If $\Re(s) > 1$ then we have

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

Recall $s = \sigma + it$, and for $\sigma > 1$ we have

$$\log^* \zeta(\sigma + it) = -\sum_p \log\left(1 - \frac{1}{p^{\sigma+it}}\right)$$

where log indicates the principal branch and $\log^*$ indicates some branch of the logarithm. By the power series expansion for log,

$$\log^* \zeta(\sigma + it) = -\sum_p \sum_{n=1}^{\infty} \frac{p^{-n(\sigma+it)}}{n}$$

Recall for $z \in \mathbb{C} \setminus \{0\}$ we can write $z = |z|e^{i\theta}$ for some $0 \leq \theta < 2\pi$ and $\log z = \log|z| + i\theta + 2k\pi i$ for some $k \in \mathbb{Z}$. So $\Re(\log z) = \log|z|$. Observe that $p^{-int} = e^{-int\log p} = \cos(-nt\log p) + i\sin(-nt\log p)$. Therefore

$$\log|\zeta(\sigma + it)| = \sum_p \sum_{n=1}^{\infty} \frac{p^{-n\sigma}}{n} \cos(nt\log p)$$

Note that $0 \leq 2(1+\cos\theta)^2 = 2 + 4\cos\theta + 2\cos^2\theta = 3 + 4\cos\theta + \cos 2\theta$. Thus

$$\sum_p \sum_{n=1}^{\infty} \frac{p^{-n\sigma}}{n}(3 + 4\cos(nt\log p) + \cos 2(nt\log p)) \geq 0$$

and so

$$3\log|\zeta(\sigma)| + 4\log|\zeta(\sigma + it)| + \log|\zeta(\sigma + i2t)| \geq 0$$

which implies

$$|\zeta(\sigma)|^3|\zeta(\sigma + it)|^4|\zeta(\sigma + i2t)| \geq 1$$

Suppose that $1 + it_0$ is a zero of $\zeta(s)$. Since $\zeta(s)$ has a pole at $s = 1$, we see that $t_0 \neq 0$. Then there exist positive numbers c_1, c_2 and c_3 such that:

1. $|\zeta(\sigma)(\sigma - 1)| \leq c_1$ for $\sigma \in (1, 2]$, since the pole at $s = 1$ is simple.
2. $|\zeta(\sigma + it_0)(\sigma - 1)^{-1}| \leq c_2$ for $\sigma \in (1, 2]$, since $1 + it_0$ is a zero of $\zeta(s)$.
3. $|\zeta(\sigma + i2t_0)| \leq c_3$ for $\sigma \in (1, 2]$, since the only pole of $\zeta(s)$ for $\Re(s) > 0$ is $s = 1$.

Thus

$$|\zeta(\sigma)(\sigma - 1)|^3|\zeta(\sigma + it_0)(\sigma - 1)^{-1}|^4|\zeta(\sigma + i2t_0)| \leq c_1^3 c_2^4 c_3$$

and hence

$$1 \leq |\zeta(\sigma)|^3|\zeta(\sigma + it)|^4|\zeta(\sigma + i2t)| \leq c_1^3 c_2^4 c_3|\sigma - 1|$$

for every $\sigma \in (1, 2]$, a contradiction. Therefore $\zeta(s)$ has no zeros for $\Re(s) \geq 1$. □

5.4 Theorem (D.J. Newman). *Suppose that $a_n \in \mathbb{C}$ with $|a_n| \leq 1$ for $n \in \mathbb{N}$. The series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges to an analytic function $F(s)$ for $\Re(s) > 1$. If $F(s)$ can be analytically continued to $\Re(s) \geq 1$ then the series converges to $F(s)$ for $\Re(s) \geq 1$,* Proof: Let $\omega \in \mathbb{C}$ with $\Re(\omega) = 1$. Then $F(z+\omega)$ is analytic for $\Re(z) \geq 0$. Let $R > 1$ and choose $\delta = \delta(R) \leq 1$ so that $F(z+\omega)$ is analytic on the region $\{x \in \mathbb{C} \mid \Re(z) \geq -\delta, |z| \leq R\}$. This region is compact, so let $M = M(R,\delta)$ be the maximum value of $F(z+\omega)$ on this region. Let Γ be the contour obtained by traversing the boundry of the region in a counterclockwise direction. Let A be the part of Γ in the right half plane and let B be the rest of Γ. By Cauchy's residue theorem,

$$2\pi i F(\omega) = \int_\Gamma F(z+\omega)\frac{1}{z}dz = \int_\Gamma F(z+\omega)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)dz$$

Note that on A, $F(z+\omega)$ is represented by the series $\sum_{n=1}^{\infty}\frac{a_n}{n^{z+\omega}}$ and we split the series into two parts. Let $N \in \mathbb{N}$ and put $S_N(z+\omega) = \sum_{n=1}^{N}\frac{a_n}{n^{z+\omega}}$ and $R_N(z+\omega) = F(z+\omega) - S_N(z+\omega)$. Again by Cauchy's residue theorem,

$$2\pi i S_N(\omega) = \int_{|z|=R} S_N(z+\omega)\frac{1}{z}dz = \int_{|z|=R} S_N(z+\omega)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)dz$$

Let C be the contour $|z| = R$ traversed in the counterclockwise direction and let A be the open right semicircle of radius R, so that $C = A \cup -A \cup \{iR\} \cup \{-iR\}$.

$$\begin{aligned}2\pi i S_N(\omega) &= \int_A S_N(z+\omega)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)dz + \int_{-A} S_N(z+\omega)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)dz\\ &= \int_A (S_N(z+\omega)N^z + S_N(\omega-z)N^{-z})\left(\frac{1}{z}+\frac{z}{R^2}\right)dz\end{aligned}$$

Thus $2\pi i(F(\omega) - S_N(\omega)) = \int_B F(z+\omega)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)dz + \int_A (R_N(z+\omega)N^z - S_N(\omega-z)N^{-z})\left(\frac{1}{z}+\frac{z}{R^2}\right)dz.$

We will now prove that $S_N(\omega) \to F(\omega)$ as $N \to \infty$. Note that for $z = x + iy$,

1. If $z \in A$ we have $\frac{1}{z}+\frac{z}{R^2} = \frac{\bar{z}}{z\bar{z}}+\frac{z}{R^2} = \frac{z+\bar{z}}{R^2} = \frac{2x}{R^2}$.
2. $|R(z+\omega)| \leq \sum_{n=N+1}^{\infty}\frac{1}{n^{x+1}} \leq \int_N^\infty \frac{1}{u^{x+1}}du = \frac{1}{xN^x}$.
3. $|S_N(\omega - z)| \leq \sum_{n=1}^{N} n^{x-1} \leq N^{x-1} + \int_0^N u^{x-1}du = N^{x-1} + \frac{N^x}{x} = N^x\left(\frac{1}{N}+\frac{1}{x}\right)$.

Therefore

$$\begin{aligned}\left|\int_A (R_N(z+\omega)N^z - S_N(\omega-z)N^{-z})\left(\frac{1}{z}+\frac{z}{R^2}\right)dz\right| &\leq \int_A \left(\left|\frac{1}{x}\right| + \left|\frac{1}{N}+\frac{1}{x}\right|\left|\frac{2x}{R^2}\right|\right)dz\\ &\leq \int_A \frac{4}{R^2}+\frac{2}{NR}dz\\ &\leq \pi R\left(\frac{4}{R^2}+\frac{2}{NR}\right)\\ &= \frac{4\pi}{R}+\frac{2\pi}{N}\end{aligned}$$

And

$$\begin{aligned}\left|\int_B F(z+\omega)N^z\left(\frac{1}{z}+\frac{z}{R^2}\right)dz\right| &\le \int_B |F(z+\omega)||N^z|\left|\frac{1}{z}+\frac{z}{R^2}\right|dz \\ &\le \int_B MN^x\left|\frac{1}{z}+\frac{z}{R^2}\right|dz \\ &\le \int_{-R}^{R} MN^\delta\frac{2}{\delta}dy+2\int_{-\delta}^{0}MN^x\frac{2x}{R^2}(2dx) \\ &\le \frac{4RM}{\delta N^\delta}+\frac{8M}{R^2}\int_{-\delta}^{0}|x|N^x dx \\ &\le \frac{4RM}{\delta N^\delta}+\frac{8M}{R^2}\frac{1}{\log N}\end{aligned}$$

Since, on the line segment $\Re(z)=\delta$, $|z|\le R$, we have $|\frac{1}{z}+\frac{z}{R^2}|\le\frac{1}{\delta}(1+\frac{1}{R})\le\frac{2}{\delta}$. Therefore

$$|2\pi i(F(\omega)-S_N(\omega))|\le\frac{4\pi}{R}+\frac{2\pi}{N}+\frac{4RM}{\delta N^\delta}+\frac{8M}{R^2\log N}$$

which goes to zero for any fixed R as $N\to\infty$. □

6 Proof of the Prime Number Theorem

Recall the Möbius function defined by

$$\mu(n)=\begin{cases}1 & \text{if } n=1\\ (-1)^k & \text{if } n \text{ is squarefree and } k \text{ is the number of distinct prime factors of } n\\ 0 & \text{otherwise}\end{cases}$$

6.1 Lemma.

$$\sum_{k|n}\mu(k)=\begin{cases}1 & \textit{if } n=1\\ 0 & \textit{if } n>1\end{cases}$$

PROOF: Plainly, $\sum_{k|1}\mu(k)=\mu(1)=1$. Suppose that n has r distinct prime factors $p_1,\dots,p_r$. Then

$$\sum_{k|n}\mu(k)=\sum_{k|p_1\dots p_r}=1-r+\binom{r}{2}-\frac{r}{3}+\dots+(-1)^r=(1-1)^r=0$$

□

6.2 Theorem (Möbius Inversion).

1. *Let $f:\mathbb{R}^+\to\mathbb{C}$ and define $F:\mathbb{R}^+\to\mathbb{C}$ by $F(x)=\sum_{n\le x}f(\frac{x}{n})$. Then*

$$f(x)=\sum_{n\le x}\mu(n)F\left(\frac{x}{n}\right)$$

2. *Let $f : \mathbb{Z}^+ \to \mathbb{C}$ and define $F : \mathbb{Z}^+ \to \mathbb{C}$ by $F(n) = \sum_{d|n} f(d) = \sum_{d|n} f(\frac{n}{d})$. Then*

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

PROOF: By Lemma 6.1,

$$f(x) = \sum_{n \le x} \left(\sum_{k|n} \mu(k) \right) f\left(\frac{x}{n}\right) \sum_{kl \le x} \mu(k) f\left(\frac{x}{kl}\right) = \sum_{k \le x} \mu(k) \left(\sum_{l \le \frac{x}{k}} f\left(\frac{x}{kl}\right) \right) = \sum_{k \le x} \mu(k) F\left(\frac{x}{k}\right)$$

For the second part,

$$f(n) = \sum_{c|n} \left(\sum_{d|\frac{n}{c}} \mu(d) \right) f(c) = \sum_{cd|n} \mu(d) f(c) = \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} f(c) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

□

6.3 Theorem.

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0$$

PROOF: For $\Re(s) > 1$, $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ represents an analytic function. But note that for $\Re(s) > 1$,

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_p \left(1 - \frac{1}{p^s} \right) = \frac{1}{\zeta(s)}$$

By Theorems 5.1 and 5.3, $(s-1)\zeta(s)$ is a non-zero analytic function for $\Re(s) \ge 1$. Hence $\frac{1}{(s-1)\zeta(s)}$ is analytic and non-zero for $\Re(s) \ge 1$, so $\frac{1}{\zeta(s)}$ is analytic and non-zero for $\Re(s) \ge 1$, $s \ne 1$. Thus by Newman's theorem, $\frac{1}{\zeta(s)}$ is represented by $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ for $\Re(s) \ge 1$. In particular, since $\lim_{s \to 1} \frac{1}{\zeta(s)} = 0$ we see that $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 0$. □

6.4 Theorem.

$$\sum_{n \le x} \mu(n) = o(x)$$

PROOF: We apply Abel summation with $a_n = \frac{\mu(n)}{n}$ and $f(x) = x$. Then $A(u) = \sum_{n \le u} \frac{\mu(n)}{n} = o(1)$ by Theorem 6.3. Thus

$$\sum_{n \le x} \mu(n) = A(x)x - \int_1^x A(u) du = o(x) - o(x) = o(x)$$

□

6.5 Definition. For any $n \in \mathbb{N}$ let $d(n)$ denote the number of postive divisors of n.

6.6 Theorem.

$$\sum_{m=1}^{n} d(m) = \sum_{m=1}^{n} \left[\frac{n}{m} \right] = n \log n + (2\gamma - 1)n + O(\sqrt{n})$$

where γ is Euler's constant.

PROOF: Consider the hyperbola $xy = n$, and let D_n be the region with $x \geq 0$, $y \geq 0$, and $xy \leq n$. The integer points (a, b) in D_n correspond to the divisors of $ab \leq n$. Thus $\sum_{m=1}^{n} d(m) = \sum_{m=1}^{n} \left[\frac{n}{m}\right]$. It remains to evaluate $\sum_{m=1}^{n} \left[\frac{n}{m}\right]$. Notice that the number of integer points in the region D_n that lie above the line $y = x$ is the same as the number of points below. Thus

$$\sum_{m=1}^{n} d(n) = [\sqrt{n}]+2\sum_{m=1}^{[\sqrt{n}]}\left[\frac{n}{m}\right]-[m] = O(\sqrt{n})+2\sum_{m=1}^{[\sqrt{n}]}\left(\frac{n}{m}-m\right)+O(\sqrt{n}) = 2n\sum_{m=1}^{[\sqrt{n}]}\frac{1}{m}-[\sqrt{n}]([\sqrt{n}]+1)+O(\sqrt{n})$$

By Theorem 4.4, $\sum_{m=1}^{[\sqrt{n}]} \frac{1}{m} = \log[\sqrt{n}] + \gamma + O(\frac{1}{\sqrt{n}})$, so

$$\begin{aligned} 2n\sum_{m=1}^{[\sqrt{n}]}\frac{1}{m} - [\sqrt{n}]([\sqrt{n}]+1) + O(\sqrt{n}) &= 2n\log(\sqrt{n}-\{\sqrt{n}\}) + 2\gamma n + O(\sqrt{n}) - (\sqrt{n}-\{\sqrt{n}\})(\sqrt{n}+1-\{\sqrt{n}\}) \\ &= 2n\log(\sqrt{n}-\{\sqrt{n}\}) + (2\gamma-1)n + O(\sqrt{n}) \\ &= n\log n + (2\gamma-1)n + O(\sqrt{n}) \end{aligned}$$

Fill in the detail. □

6.7 Theorem (Prime Number Theorem).

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

PROOF: By Theorem 4.1 it suffices to show that $\psi(x) \sim x$. Put

$$F(x) = \sum_{n \leq x}\left(\psi\left(\frac{x}{n}\right) - \left[\frac{x}{n}\right] + 2\gamma\right)$$

By Möbius inversion, Theorem 6.2, $\psi(x) - [x] + 2\gamma = \sum_{n \leq x} \mu(n)F(\frac{x}{n})$, and so it suffices to show that $\sum_{n \leq x} \mu(n)F(\frac{x}{n}) = o(x)$. Now

$$\begin{aligned} \sum_{n \leq x}\psi\left(\frac{x}{n}\right) &= \sum_{n \leq x}\sum_{m \leq \frac{x}{n}} \Lambda(m) \\ &= \sum_{m \leq x}\Lambda(m)\sum_{m \leq \frac{x}{m}} 1 \\ &= \sum_{m \leq x}\Lambda(m)\left[\frac{x}{m}\right] \\ &= \sum_{p \leq x}(\log p)\left(\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \cdots\right) \\ &= \log([x]!) = x\log x - x + O(\log x) \end{aligned}$$

By Theorem 6.6,

$$\sum_{n \leq x}\left[\frac{[x]}{n}\right] = [x]\log[x] + (2\gamma-1)[x] + O(\sqrt{x})$$

Notice that

$$\sum_{n \leq x}\left[\frac{[x]}{n}\right] \leq \sum_{n \leq x}\left[\frac{x}{n}\right] \leq \sum_{n \leq x+1}\left[\frac{[x]+1}{n}\right]$$

Therefore $\sum_{n\le x}\left[\frac{x}{n}\right] = x\log x + (2\gamma-1)x + O(\sqrt{x})$, and so $F(x) = \sum_{n\le x}\left(\psi\left(\frac{x}{n}\right) - \left[\frac{x}{n}\right] + 2\gamma\right) = O(\sqrt{x})$. Let $c>0$ be such that $|F(x)| < c\sqrt{x}$ for all $x \ge 1$. Let $t \ge 2$ be a real number. Then

$$\left|\sum_{n\le\frac{x}{t}}\mu(n)F\left(\frac{x}{n}\right)\right| \le \sum_{n\le\frac{x}{t}}\left|F\left(\frac{x}{n}\right)\right| \le \sum_{n\le\frac{x}{t}} c\sqrt{\frac{x}{n}} \le c\sqrt{x}\sum_{n\le\frac{x}{t}}\frac{1}{\sqrt{n}} \le x\sqrt{x}\sqrt{\frac{x}{t}} = c\frac{x}{\sqrt{t}}$$

Since F is a step function with jumps only at integer points, $F(x) = F([x])$ for all $x \ge 1$. We see that

$$\sum_{\frac{x}{t}<n\le x}\mu(n)F\left(\frac{x}{n}\right) = F(1)\sum_{\frac{x}{2}<n\le x}\mu(n) + F(2)\sum_{\frac{x}{3}<n\le\frac{x}{2}}\mu(n) + \cdots + F([t])\sum_{\frac{x}{t}<n\le\frac{x}{[t]}}\mu(n)$$

Therefore

$$\begin{aligned}\left|\sum_{\frac{x}{t}<n\le x}\mu(n)F\left(\frac{x}{n}\right)\right| &\le (|F(1)+\cdots+|F([t])|)\left(\left|\sum_{\frac{x}{2}<n\le x}\mu(n)\right| + \cdots + \left|\sum_{\frac{x}{t}<n\le\frac{x}{[t]}}\mu(n)\right|\right)\\ &\le (|F(1)+\cdots+|F([t])|)o(x)\end{aligned}$$

since $\sum_{n\le x}\mu(n) = o(x)$. Given $\varepsilon > 0$ choose t so large that $\frac{c}{\sqrt{t}} < \frac{\varepsilon}{2}$ and then take x sufficiently large that $|\sum_{\frac{x}{t}<n\le x}\mu(n)F\left(\frac{x}{n}\right)| < \frac{\varepsilon}{2}x$, so that $|\sum_{n\le x}\mu(n)F\left(\frac{x}{n}\right)| < \varepsilon x$. The proof is complete. □

$\mathrm{Li}(x) = \int_2^x \frac{du}{\log u}$ is a better approximation to $\pi(x)$ than $\frac{x}{\log x}$. In fact, $\pi(x) = \mathrm{Li}(x) + O(x\exp(-c(\log x)^{\frac{3}{5}}))$ has been proved. Littlewood proved that there are $c_1, c_2 > 0$ such that for infinitely many integers x, $\pi(x) - \mathrm{Li}(x) > c_1\frac{\sqrt{x}}{\log x}\log\log\log x$ and $\mathrm{Li}(x) - \pi(x) > c_2\frac{\sqrt{x}}{\log x}\log\log\log x$. Initial calculation suggests that $\mathrm{Li}(x) > \pi(x)$ for all x. Skewes in 1955 showed that there exists x_0 for which $\pi(x_0) > \mathrm{Li}(x_0)$ with $x_0 < 10^{10^{10^{964}}}$. In 1966 Lehmann lowered the bound to 10^{1166}. Probably $\mathrm{Li}(x) > \pi(x)$ for $x < 10^{20}$.

7 Generalizing $\pi(x)$

7.1 Definition. For any positive integer n, let $\Omega(n)$ denote the number of prime factors of n, counted with multiplicity. Let $\omega(n)$ denote the number of distinct prime factors of n. For each $k \in \mathbb{Z}$ let $\tau_k(x)$ denote the number of positive integers $n \le x$ with $\Omega(n) = k$. Let $\pi_k(x)$ denote the number of positive integers $n \le x$ for which $\Omega(n) = \omega(n) = k$.

Note that $\pi(x) = \pi_1(x) = \tau_1(x)$.

7.2 Theorem (Landau, 1900). *Let $k \in \mathbb{N}$. Then*

$$\pi_k(x) \sim \tau_k(x) \sim \frac{1}{(k-1)!}\frac{x}{\log x}(\log\log x)^{k-1}$$

Proof: We'll prove the result by induction on k. The case $k = 1$ is the Prime Number Theorem. We introduce the functions $L_k(x)$, $\Pi_k(x)$, and $\theta_k(x)$, which are defined by

$$L_k(x) = \sideset{}{^*}\sum_{p_1\cdots p_k\le x}\frac{1}{p_1\cdots p_k} \qquad \Pi_k(x) = \sideset{}{^*}\sum_{p_1\cdots p_k\le x} 1 \qquad \Theta_k(x) = \sideset{}{^*}\sum_{p_1\cdots p_k\le x}\log(p_1\cdots p_k)$$

The star indicates that the sum is taken over all k-tuples $(p_1, \cdots, p_k)$ of primes with $p_1 \cdots p_k \le x$. Observe that more than one such k-tuple may be associated with the same product. For each integer n let $c_n = c_n(k)$ denote the number of k-tuples whose product is n. Thus if $\Omega(n) = \omega(n) = k$ then $c_n = k!$ since n is a product of k distinct primes. Similarily, if $\Omega(n) = k$ then $c_n \le k!$, and if $\Omega(n) \ne k$ then $c_n = 0$. It follows that $\Pi_k(x) = \sum_{n \le x} c_n$ and $\theta_k(x) = \sum_{n \le x} c_n \log n$. Further observe that

$$k!\pi_k(x) \le \Pi_k(x) \le k!\tau_k(x)$$

For $k \ge 2$, the number of integers $n \le x$ for which $\Omega(n) = k$ and $\omega(n) \ne k$ is $\tau_k(x) - \pi_k(x)$. In particular,

$$\tau_k(x) - \pi_k(x) \le \sideset{}{^*}\sum_{\substack{p_1 \cdots p_k \le x \\ p_i = p_j \text{ for some} \\ (i,j) \text{ with } i \ne j}} 1 \le \binom{k}{2} \sideset{}{^*}\sum_{q_1 \cdots q_{k-1} \le x} 1 = \binom{k}{2} \Pi_{k-1}(x)$$

Thus it suffices to show that $\Pi_k(x) \sim k\frac{x}{\log x}(\log\log x)^{k-1}$. For fixed $k \ge 2$, apply Abel summation with $a_n = c_n$ and $f(x) = \log x$. Then

$$\begin{aligned}
\Theta_k(x) &= \sum_{n \le x} c_n \log n = \left(\sum_{n \le x} c_n\right) \log x - \int_1^x \frac{\sum_{n \le u} c_n}{u} du \\
&= \Pi_k(x) \log x - \int_1^x \frac{\Pi_k(u)}{u} du \\
&= \Pi_k(x) \log x + O(x) && \text{since } \Pi_k(u) \le k!u
\end{aligned}$$

Observe that $\Theta_1(x) = \theta(x)$, and so by Theorem 4.1 and the Prime Number Theorem, $\Theta_1(x) \sim x$. We shall now assume that $k \ge 2$ and that $\Theta_j(x) \sim jx(\log\log x)^{j-1}$ for $1 \le j < k$. This is our induction hypothesis.

By Theorem 4.7, $\sum_{p \le x} \frac{1}{p} \sim \log\log x$. Since

$$\left(\sum_{p \le x^{\frac{1}{k}}} \frac{1}{p}\right)^k \le L_k(x) \le \left(\sum_{p \le x} \frac{1}{p}\right)^k$$

we get that $L_k(x) \sim (\log\log x)^k$. We can write Θ_k and L_k in terms of Θ_{k-1} and L_{k-1}, respectively:

$$\begin{aligned}
(k-1)\Theta_k(x) &= \sideset{}{^*}\sum_{p_1 \cdots p_k \le x} (k-1) \log(p_1 \cdots p_k) \\
&= \sideset{}{^*}\sum_{p_1 \cdots p_k \le x} \log(p_1 \cdots p_{k-1}) + \log(p_1 \cdots p_{k-2} p_k) + \cdots + \log(p_2 \cdots p_k) \\
&= k \sideset{}{^*}\sum_{p_1 \cdots p_k \le x} \log(p_2 \cdots p_k) \\
&= k \sum_{p_1 \le x} \Theta\left(\frac{x}{p_1}\right)
\end{aligned}$$

and

$$L_k(x) = \sideset{}{^*}\sum_{p_1 \cdots p_k \le x} \frac{1}{p_1 \cdots p_k} = \sum_{p_1 \le x} \frac{1}{p_1} L_{k-1}\left(\frac{x}{p_1}\right)$$

By our induction hypothesis, $\Theta_{k-1}(x)-(k-1)xL_{k-2}(x)=o(x(\log\log x)^{k-2})$. Given any $\varepsilon>0$, there is $x_0=x_0(k,\varepsilon)$ such that $|\Theta_{k-1}(x)-(k-1)xL_{k-2}(x)|<\varepsilon x(\log\log x)^{k-2}$ for all $x>x_0$. Let c be such that $|\Theta_{k-1}(x)-(k-1)xL_{k-2}(x)|<c$ for all $x\le x_0$. Then

$$\begin{aligned}
|\Theta_k(x)-kxL_{k-1}(x)| &= \frac{k}{k-1}\left|\sum_{p\le x}\Theta_{k-1}\left(\frac{x}{p}\right)-(k-1)\frac{x}{p}L_{k-2}\left(\frac{x}{p}\right)\right| \\
&\le 2\sum_{p\le x}\left|\Theta_{k-1}\left(\frac{x}{p}\right)-(k-1)\frac{x}{p}L_{k-2}\left(\frac{x}{p}\right)\right| \\
&\le 2\sum_{\frac{x}{x_0}<p\le x}c+2\sum_{p\le\frac{x}{x_0}}\varepsilon\frac{x}{p}\left(\log\log\frac{x}{p}\right)^{k-2} \\
&\le 2xc+2\varepsilon x(\log\log x)^{k-2}\sum_{p\le\frac{x}{x_0}}\frac{1}{p} \\
&\le 2xc+4\varepsilon x(\log\log x)^{k-1} && \text{by Theorem 4.7} \\
&\le 5\varepsilon x(\log\log x)^{k-1} && \text{for } x \text{ sufficiently large}
\end{aligned}$$

Since $\varepsilon>0$ was arbitrary, this completes the proof by induction. □

7.3 Theorem.

$$\sum_{n\le x}\omega(n)=x\log\log x+B_1x+O\left(\frac{x}{\log x}\right)$$

$$\sum_{n\le x}\Omega(n)=x\log\log x+B_2x+o(x)$$

where $B_2=B_1+\sum_p\frac{1}{p(p-1)}$.

Proof: See online notes. □

Let $N\in\mathbb{N}$ and let $A\subseteq\{1,\dots,N\}$. Plainly, $\frac{|A|}{N}$ is a measure of the density or thickness of A in $\{1,\dots,N\}$. We extend this notion to subsets A of $\mathbb{N}$. For each integer N we denote by $A(N)$ the set $A\cap\{1,\dots,N\}$. We define the *upper density* of A, denoted $\overline{d}(A)$, by $\limsup_{N\to\infty}\frac{|A(N)|}{N}$. The *lower density* of A, $\underline{d}(A)$, is defined as $\liminf_{N\to\infty}\frac{|A(N)|}{N}$. If $\overline{d}(A)=\underline{d}(A)$ then we put $d(A)$ to be this quantity and say that A has asymtotic density $d(A)$.

7.4 Example.

1. Note that the even integers have density $\frac{1}{2}$.
2. Put $A=\{n\in\mathbb{N}\mid 10^{2k-1}\le n<10^{2k}, k=1,2,\dots\}$. Note that $\frac{A(10^{2k-1})}{10^{2k-1}}\le\frac{10^{2k-2}}{10^{2k-1}}=\frac{1}{10}$, while $\frac{A(10^{2k})}{10^{2k}}\ge\frac{10^{2k}-10^{2k-1}}{10^{2k}}=\frac{9}{10}$. Hence A does not have an asymtotic density.

Let $f,F:\mathbb{N}\to\mathbb{R}$. We say that f has *normal order* F if for each $\varepsilon>0$ the set $A(\varepsilon)=\{n\in\mathbb{N}\mid(1-\varepsilon)F(n)<f(n)<(1+\varepsilon)F(n)\}$ has density 1. Note that if we put $B(\varepsilon)=\mathbb{N}\setminus A(\varepsilon)$ then $\overline{d}(B(\varepsilon))=0$.

7.5 Example.

1. Let $f(x)=\pi(x)$ and $F(x)=\frac{x}{\log x}$. By the Prime Number Theorem, $\pi(x)$ has normal order $\frac{x}{\log x}$.
2. For any function f, it has normal order of itself.

7.6 Theorem (Turan). *Let $\delta > 0$. The number of integers $n \le x$ for which*

$$|\omega(n) - \log\log n| > (\log\log n)^{\frac{1}{2}+\delta}$$

is $o(x)$ and the number of integers $n \le x$ for which

$$|\Omega(n) - \log\log n| > (\log\log n)^{\frac{1}{2}+\delta}$$

is $o(x)$.

PROOF: This proof is incomplete. □

7.7 Theorem. *Let $\varepsilon > 0$. Then*

$$2^{(1-\varepsilon)\log\log n} < d(n) < 2^{(1+\varepsilon)\log\log n}$$

on a set of postive integers with asymtotic density one.

PROOF: Exercise. □

8 Law of Quadratic Reciprocity

8.1 Definition. For any $n \in \mathbb{N}$, let $\varphi(n)$ denote the number of invertible equivalence classes in the ring $\mathbb{Z}/n\mathbb{Z}$. φ is known as *Euler's totient function*.

8.2 Theorem (Euler). *Let a and n be positvie integers with* $\gcd(a,n) = 1$. *Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

PROOF: Let $c_1, \dots, c_{\varphi(n)}$ be all of the intvertible elements modulo n. Then since a is invertible, the collection $ac_1, \dots, ac_{\varphi(n)}$ is also all of the invertible elements modulo n. Therefore $c_1 \cdots c_{\varphi(n)} \equiv (ac_1)\cdots(ac_{\varphi(n)} \pmod{n}$, so $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

The special case of Euler's Theorem where n is prime is known as Fermat's Little Theorem.

8.3 Theorem (Wilson). *If p is prime then $(p-1)! \equiv -1 \pmod{p}$.*

PROOF: By Fermat's Little Theorem $x^{p-1} - 1$ factors as $(x-1)\cdots(x-(p-1))$ in $(\mathbb{Z}/p\mathbb{Z})[x]$. Therefore, by comparing constant coefficients, $-1 \equiv (-1)^{p-1}(p-1)! \pmod{p}$. The result follows. □

Wilson's Theorem was conjectured by Wilson (1741-1793). He communicated the conjecture to Waring (1734-1798), who pbulished it in 1770. Shortly afterwards, Lagrange gave the first proof. In fact, Leibniz had conjectured the result in 1682. Here is a proof due to Stern in 1860. For $|x| < 1$,

$$\log\left(\frac{1}{1-x}\right) = -\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots$$

and so

$$\exp\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots\right) = \frac{1}{1-x} = 1 + x + x^2 + \cdots$$

But

$$\begin{aligned}\exp\left(x+\frac{x^2}{2}+\frac{x^3}{3}+\cdots\right) &= \exp(x)\exp\left(\frac{x^2}{2}\right)\exp\left(\frac{x^3}{3}\right)\cdots \\ &= 1+x+\left(\frac{1}{2!}+\frac{1}{2}\right)x^2+\left(\frac{1}{3!}+\frac{1}{2}+\frac{1}{3}\right)x^3+\cdots+\left(\frac{1}{p!}+\cdots+\frac{1}{p}\right)x^p+\cdots\end{aligned}$$

In particular, the coefficient of x^p can be written $\frac{1}{p!}+\frac{r}{s}+\frac{1}{p}$, where $\frac{r}{s}$ is in lowest terms and s is coprime with p. Comparing coefficients in the power series shows that

$$\begin{aligned} 1 &= \frac{1}{p!}+\frac{r}{s}+\frac{1}{p} \\ s-r &= \frac{s}{p!}+\frac{s}{p} \\ (s-r)(p-1)! &= \frac{s((p-1)!+1)}{p}\end{aligned}$$

Now $(s-r)(p-1)!$ is an integer, so $p \mid s((p-1)!+1)$. But $\gcd(s,p)=1$, so $p \mid (p-1)!+1$, as required.

8.4 Definition. Let p be a prime and a an integer coprime with p. The *Legendre symbol* is defined to be

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & \text{otherwise}\end{cases}$$

If $(\frac{a}{p})=1$ then we say that a is a *quadratic residue modulo* p, otherwise we say that a is a *quadratic nonresidue modulo* p.

8.5 Theorem (Euler's Criterion). *Let p be an odd prime and let a be an integer coprime with p. Then*

$$a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \pmod{p}$$

Proof: The congruence $x^2 \equiv a \pmod{p}$ has a most 2 solutions modulo p since $\mathbb{Z}/p\mathbb{Z}$ is a field. Suppose that it has a solution $x=b$. Then

$$a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv 1 \equiv (\frac{a}{p}) \pmod{p}$$

On the other hand, suppose that there is no such solution. We may partition $\mathbb{Z}/p\mathbb{Z}$ into pairs (r,s) such that $rs \equiv a \pmod{p}$. Then by Wilson's Theorem, $-1 \equiv (p-1)! = a^{\frac{p-1}{2}} \pmod{p}$, as required. □

Let us extend the definition of the Legendre symbol $(\frac{a}{p})$ to include the case where $p \mid a$. In this case, define $(\frac{a}{p})=0$.

8.6 Theorem. *Let p be an odd prime and let a and b be integers. Then*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$$

and $(\frac{-1}{p})=(-1)^{\frac{p(p-1)}{2}}$.

PROOF: The second part holds by Euler's Criterion since $(-1)^p = -1$. If $p \mid ab$ then the first part clearly holds. Suppose that $p \nmid ab$. By Euler's Criterion

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

Since p is an odd prime and the Legendre symbols take on values in $\{1, -1\}$, the result follows. □

8.7 Theorem (Gauß Lemma). *Let p be an odd prime and a an integer coprime with p. Let μ be the number of integers from $a, 2a, \dots, \frac{p-1}{2}a$ whose residue modulo p of least absolute value is negative. Then $(\frac{a}{p}) = (-1)^\mu$.*

PROOF: Replace the numbers $a, 2a, \dots, \frac{p-1}{2}a$ be their residues of least absolute value, say by $r_1, \dots, r_{\frac{p-1}{2}-\mu}$ and $-s_1, \dots, -s_\mu$, where the r_i's and s_j's are positive. Plainly, the r_i's are all distinct and the s_j's are all distinct. Suppose that $r_i = s_j$ for some i and j. Then $m_1 a \equiv r_i \pmod p$ and $m_2 \equiv s_j \pmod p$ for distinct integers $1 \le m_1, m_2 \le \frac{p-1}{2}$. But then $(m_1 + m_2)a \equiv 0 \pmod p$, and since $p \nmid a$, $p \mid m_1 + m_2$. But $2 \le m_1 + m_2 \le p - 1$, a contradiction. Therefore the r_i's and s_j's are all distinct, so they are a rearrangement of the numbers $1, \dots, \frac{p-1}{2}$. Accordingly, $a(2a)\cdots(\frac{p-1}{2}a) \equiv (\frac{p-1}{2})!(-1)^\mu \pmod p$, so $a^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod p$. Then $(\frac{a}{p}) = (-1)^\mu$ by Euler's Criterion. □

8.8 Corollary. *Let p be an odd prime. Then $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.*

PROOF: By Gauß' Lemma, $(\frac{2}{p}) = (-1)^\mu$, where μ is the number of the first $\frac{p-1}{2}$ multiples of 2 which lie in the range $[\frac{p}{2}, p-1]$. We now check what happens when $p \equiv 1, 3, 5, 7 \pmod 8$ in turn. If $p = 8k+1$ then $\mu = \frac{p-1}{2} - [\frac{p}{4}] = 2k$. If $p = 8k+3$ or $8k+5$ then by the same formula $\mu = 2k+1$. Finally, if $p = 8k+7$ then $\mu = 2k+2$. The result follows. □

8.9 Proposition. *Let p be an odd prime and a an integer coprime with $2p$. Then $(\frac{a}{p}) = (-1)^t$ where $t = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right]$.*

PROOF: We let $r_1, \dots, r_{\frac{p-1}{2}-\mu}$ and $-s_1, \dots, -s_\mu$, as before, be the residues of least absolute value modulo p of the integers $a, 2a, \dots, \frac{p-1}{2}a$, where the r_i's and s_j's are positive. Notice that if $1 \le j \le \frac{p-1}{2}$ then $ja = p[\frac{ja}{p}] + \ell_j$, where $0 \le \ell_j < p$. So ℓ_j is either r_k for some $1 \le k \le \frac{p-1}{2} - \mu$ or is it $p - s_k$ for some $1 \le k \le \mu$. Thus

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] + \ell_j = p\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{ja}{p}\right] + \sum_{j=1}^{\frac{p-1}{2}} \ell_j$$

But

$$\begin{aligned}
\sum_{j=1}^{\frac{p-1}{2}} \ell_j &= r_1 + \cdots + r_{\frac{p-1}{2}-\mu} + p\mu - (s_1 + \cdots + s_\mu) \\
&= (r_1 + \cdots + r_{\frac{p-1}{2}-\mu} + s_1 + \cdots + s_\mu) + p\mu - 2(s_1 + \cdots + s_\mu) \\
&= (1 + 2 + \cdots + \frac{p-1}{2}) + p\mu - 2(s_1 + \cdots + s_\mu)
\end{aligned}$$

Therefore

$$\sum_{j=1}^{\frac{p-1}{2}} ja - \sum_{j=1}^{\frac{p-1}{2}} j = p\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + p\mu - 2(s_1 + \cdots + s_\mu)$$

$$(a-1)\frac{\frac{p-1}{2}\frac{p+1}{2}}{2} = p\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + p\mu - 2(s_1 + \cdots + s_\mu)$$

Since a is odd, $a-1$ is even, so $0 \equiv p\mu + p\sum_{j=1}^{\frac{p-1}{2}}[\frac{ja}{p}] \pmod 2$, so $\mu \equiv \sum_{j=1}^{\frac{p-1}{2}}[\frac{ja}{p}] \pmod 2$, as required. □

8.10 Theorem (Law of Quadratic Reciprocity). *If p and q are distinct primes then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$$

Euler stated the law. Legendre attempted to prove it. Gauß gave 8 proofs.

Proof: By Gauß' Lemma, $(\frac{q}{p}) = (-1)^\mu$ and $(\frac{p}{q}) = (-1)^\nu$, where μ and ν are the number of integers from $\{q, 2q, \dots, \frac{p-1}{2}q\}$ and $\{p, 2p, \dots, \frac{q-1}{2}p\}$, respectively, whose residue modulo p and q, respectively, of least absolute value is negative. It suffices to show that $\mu + \nu \equiv (\frac{p-1}{2})(\frac{q-1}{2}) \pmod 2$. Given x with $1 \le x \le \frac{p-1}{2}$, let y be such that $-\frac{p}{2} < qx - py < \frac{p}{2}$. Notice that $-\frac{1}{2} - \frac{q}{p}x < -y < \frac{1}{2} - \frac{q}{p}x$, so y is uniquely determined. Then $qx - py$ is the residue of qx modulo p of least absolute value. y is non-negative, and if $y = 0$ then there is no contribution to μ since $qx \ge 0$. Further, if $x = \frac{p-1}{2}$ then

$$y < \frac{q}{p}x + \frac{1}{2} = \frac{q}{2}\left(\frac{p-1}{p}\right) + \frac{1}{2}$$

Therefore $y \le \frac{q-1}{2}$ since it is an integer. It follows that μ corresponds to the number of combinations of x and y from the sequences $1, 2, \dots, \frac{p-1}{2}$ and $1, 2, \dots, \frac{q-1}{2}$, repectively, such that $-\frac{p}{2} < qx - py < 0$. Similarily, ν is the number of combinations such that $-\frac{q}{2} < py - qx < 0$. For any pair (x, y) with $1 \le x \le \frac{p-1}{2}$ and $1 \le y \le \frac{q-1}{2}$, either $py - qx < -\frac{q}{2}$ or $py - qx > \frac{p}{2}$. Let ρ be the number of pairs for which the former holds and λ be the number of pairs for which the latter holds. Then

$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = \mu + \nu + \rho + \lambda$$

As x and y run through their respective domains, $x' = \frac{p+1}{2} - x$ and $y' = \frac{q+1}{2} - y$ fun through the same domains, but in reverse order. Notice that $py - qx > \frac{p}{2}$ if and only if $py' - qx' = \frac{p-q}{2} - (py - qx) < -\frac{q}{2}$. By symmetry, $py - qx < -\frac{q}{2}$ if and only if $py' - qx' > \frac{p}{2}$. Therefore $\lambda = \rho$ and so $\mu + \nu \equiv (\frac{p-1}{2})(\frac{q-1}{2}) \pmod 2$, and the result is proven. □

8.11 Example. Let $k \in \mathbb{N}$. The equation $y^2 = x^3 + k$ is known as Mordell's equation. Here we are looking for solutions in integers x and y. There are only finitely many solutions in the integers for any fixed k. In general, it is not easy to find all solutions However, in about 1970, Harold Stark proved that for each $\varepsilon > 0$ there exists a positive number $c(\varepsilon) > 0$, such that if (x, y) is a solution in the integers, then $|x|, |y| < e^{c(\varepsilon)k^{1+\varepsilon}}$.

For some k, all solutions can be found by congruence considerations. For example, consider the equation $y^2 = x^3 + 45$. Note that if x is even then $y^2 \equiv 45 \pmod 8$, so $y^2 \equiv 5 \pmod 8$, which is not possible. Thus it $y^2 = x^3 + 45$ has a solution in the integers then x is odd. We consider the four possiblilties $x \equiv 1, 3, 5, 7 \pmod 8$. Suppose that $x \equiv 1 \pmod 8$ or $x \equiv 5 \pmod 8$. Then $x^3 \equiv 1 \pmod 4$ and so $y^2 \equiv 2 \pmod 4$, which is impossible. Suppose now that $x \equiv 7 \pmod 8$. We have $y^2 - 18 = x^3 + 27 = (x+3)(x^2 - 3x + 9)$. We claim that there is a prime $p \equiv \pm 3 \pmod 8$ such that $p \mid x^2 - 3x + 9$. This is so since if all primes dividing $x^2 - 3x + 9$ were congruent to ± 1 modulo 8 then $x^2 - 3x + 9$ would also be equivalent to ± 1 modulo 8, which it is not. Now consider the equation modulo p. We find that $y^2 \equiv 18 \pmod p$, or equivalently, $(\frac{18}{p}) = 1$. But $(\frac{18}{p}) = (\frac{2\cdot 3^2}{p}) = (\frac{2}{p}) = -1$, a contradiction. Therefore $x \equiv 3 \pmod 8$. Note that $y^2 - 2 \cdot 6^2 = x^3 - 27 = (x-3)(x^2 + 3x + 9)$. Since $x \equiv 3 \pmod 8$, $x^2 + 3x + 9 \equiv 3 \pmod 8$. As before, we see that $x^2 + 3x + 9$ is divisible by a prime $p \equiv \pm 3 \pmod 8$. It follows that $y^2 = x^3 + 45$ has no integer solutions.

8.12 Example. How does 9997 factor? We could just factor it, but we're mad keen to use the Law of Quadratic Reciprocity. Notice that $9997 = 100^2 - 3$. By the Law of Quadratic Reciprocity, if p is odd and $p \mid 9997$ then $100^2 \equiv 3 \pmod p$, so

$$1 = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$$

If $p \equiv 1 \pmod{12}$ then $(\frac{p}{3})(-1)^{\frac{p-1}{2}} = (\frac{1}{3}) = 1$. If $p \equiv 5 \pmod{12}$ then $(\frac{p}{3})(-1)^{\frac{p-1}{2}} = -1$, so this case is impossible. If $p \equiv 7 \pmod{12}$ then $(\frac{p}{3})(-1)^{\frac{p-1}{2}} = -1$, and if $p \equiv 11$ (mod 1)2 then $(\frac{p}{3})(-1)^{\frac{p-1}{2}} = 1$. Therefore if $p \mid 9997$ then $p \equiv \pm 1$ (mod 1)2. We now test 11, 13,... In fact, $9997 = 13 \cdot 769$. The same argument shows that the primes dividing 769 are ± 1 modulo 12. Clearly $\sqrt{769} < 30$, so we need only check 11, 13, 23, none of which work. Therefore 769 is prime.

9 Dirichlet's Theorem

For any pair of integers a and b not both zero, we can find, by means of the Euclidean algorithm, integers x and y for which $ax + by = \gcd(a, b)$.

9.1 Theorem (Chinese Remainder Theorem). *Let $m_1, \ldots, m_t$ be pairwise coprime positive integers. Let $m = m_1 \cdots m_t$ and $b_1, \ldots, b_t$ be any integers. The simlutaneous congruences*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ x &\equiv b_t \pmod{m_t} \end{aligned}$$

have a unique solution modulo m.

PROOF: Let $n_i = \frac{m}{m_i}$ for $1 \le i \le t$. Then note that $\gcd(n_i, m_i) = 1$, so there are integers r_i, s_i such that $r_i m_i + s_i n_i = 1$. Thus $s_i n_i \equiv 1 \pmod{m_i}$. Put $e_i = s_i n_i$ and notice that $b_i e_i \equiv b_i \pmod{m_i}$. But $n_i \equiv 0 \pmod{m_j}$ for $j \neq i$, so $b_i e_i \equiv 0 \pmod{m_j}$ for $j \neq i$. Let $x = b_1 e_1 + \cdots + b_t e_t$, a solution to the simultaneous congruences.

Suppose that x_0 and x_1 are solutions to the simultaneous congruences. Then $x_0 \equiv x_1 \pmod{m_i}$ for $i = 1, \ldots, t$. Since the m_i's are coprime, $m_1 \cdots m_t \mid x_0 - x_1$. In particular, $x_0 \equiv x_1 \pmod m$. □

9.2 Theorem. *Let $m_1, \ldots, m_t$ be pairwise coprime positive integers. Let $m = m_1 \cdots m_t$. The ring $\mathbb{Z}/m\mathbb{Z}$ is isomorphic to $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z}$ and the group $(\mathbb{Z}/m\mathbb{Z})^*$ is isomorphic to $(\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_t\mathbb{Z})^*$.*

PROOF: Let $\psi : \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z} : n \mapsto (n + m_1\mathbb{Z}, \ldots, n + m_t\mathbb{Z})$. ψ is a ring homomorphism. By the Chinese Remainder Theorem, ψ is onto. $\ker\psi = \{n \in \mathbb{Z} : m_1 \cdots m_t \mid n\} = m\mathbb{Z}$. The First Isomorphism Theorem gives us the first result.

Let $\lambda : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_t\mathbb{Z})^* : (n+m\mathbb{Z}) \mapsto (n+m_1\mathbb{Z}, \ldots, n+m_t\mathbb{Z})$. Then λ is a well defined group homomorphism. By the Chinese Remainder Theorem λ is an isomorphism. □

9.3 Corollary. *Let $m_1, \ldots, m_t$ be pairwise coprime positive integers. Let $m = m_1 \cdots m_t$. Then*

$$\varphi(m) = \varphi(m_1) \cdots \varphi(m_t)$$

Proof: $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$. □

9.4 Corollary. *Let $m \in \mathbb{N}$. Then*

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

9.5 Theorem.

$$\sum_{j=1}^{n} \varphi(j) = \frac{3}{\pi^2} n^2 + O(n \log n)$$

Proof:

$$\begin{aligned}
\sum_{j=1}^{n} \varphi(j) &= \sum_{j=1}^{n} j \prod_{p|j} \left(1 - \frac{1}{p}\right) \\
&= \sum_{j=1}^{n} j \sum_{d|j} \frac{\mu(d)}{d} \\
&= \sum_{d'd \le n} d' \mu(d) \\
&= \sum_{d=1}^{n} \mu(d) \sum_{d'=1}^{\left[\frac{n}{d}\right]} d' \\
&= \sum_{d=1}^{n} \mu(d) \frac{\left[\frac{n}{d}\right] (\left[\frac{n}{d}\right] + 1)}{2} \\
&= \frac{1}{2} \sum_{d=1}^{n} \mu(d) \left[\frac{n}{d}\right]^2 + \mu(d) \left[\frac{n}{d}\right] \\
&= \frac{1}{2} \sum_{d=1}^{n} \mu(d) \frac{n^2}{d^2} + O(n) + \frac{1}{2} \sum_{d=1}^{n} \mu(d) \frac{n}{d} + O(n) \\
&= \frac{n^2}{2} \sum_{d=1}^{n} \mu(d) \frac{1}{d^2} + O(n \log n) \\
&= \frac{n^2}{2} \sum_{d=1}^{\infty} \mu(d) \frac{1}{d^2} - \frac{n^2}{2} \sum_{d=n+1}^{\infty} \mu(d) \frac{1}{d^2} + O(n \log n) \\
&= \frac{n^2}{2} \zeta(2)^{-1} + O(n \log n) \\
&= \frac{3}{\pi^2} n^2 + O(n \log n)
\end{aligned}$$

□

If p is an odd prime and $\ell \in \mathbb{N}$ then $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ is cyclic. To prove this we'll need some preliminary results. Notice that the result does not hold if $p = 2$, as $(\mathbb{Z}/8\mathbb{Z})^*$ has order four but all of its elements have order 1 or 2.

9.6 Proposition. *Let p be a prime and ℓ a positive integer. If $a \equiv b \pmod{p^\ell}$ then $a^p \equiv b^p \pmod{p^{\ell+1}}$.*

PROOF: Since $a \equiv b \pmod{p^\ell}$ there is c such that $a = b + cp^\ell$. Then

$$a^p = (b + cp^\ell)^p = b^p + \binom{p}{1} b^{p-1} cp^\ell + \binom{p}{2} b^{p-1} (cp^\ell)^2 + \cdots + (cp^\ell)^p$$

This implies that $a^b \equiv b^p \pmod{p^{\ell+1}}$. □

9.7 Proposition. *If p is an odd prime and $\ell \geq 2$ is an integer then for any integer a,*

$$(1+ap)^{p^{\ell-2}} \equiv 1 + ap^{\ell-1} \pmod{p^\ell}$$

PROOF: By induction on ℓ. The result holds for $\ell = 2$, so suppose it holds for some $\ell \geq 2$. We have

$$(1+ap)^{p^{\ell-2}} \equiv 1 + ap^{\ell-1} \pmod{p^\ell}$$

and so by Proposition 9.6,

$$(1+ap)^{p^{\ell-1}} \equiv (1 + ap^{\ell-1})^p \pmod{p^{\ell+1}}$$

But

$$(1+ap^{\ell-1})^p = 1 + \binom{p}{1} ap^{\ell-1} + \binom{p}{2} (ap^{\ell-1})^2 + \cdots + (ap^{\ell-1})^p \equiv 1 + ap^\ell \pmod{p^{\ell+1}}$$

and the result is proved since $p^{2\ell-1}$ divides each term in the sum except for the first two. □

9.8 Proposition. *Let $\ell \in \mathbb{N}$. If p is an odd prime and a is an integer coprime with p then the order of $1 + ap + p^\ell\mathbb{Z}$ in $(\mathbb{Z}/p^\ell)^*$ is $p^{\ell-1}$.*

PROOF: The result is immediate if $\ell = 1$, so suppose that $\ell \geq 2$. By Proposition 9.7,

$$(1+ap)^{p^{\ell-2}} \equiv 1 + ap^{\ell-1} \not\equiv 0 \pmod{p^\ell}$$

and by Proposition 9.6

$$(1+ap)^{p^{\ell-1}} \equiv (1 + ap^{\ell-1})^p \pmod{p^{\ell+1}}$$

so $(1+ap)^{p^{\ell-1}} \equiv 1 \pmod{p^\ell}$. Therefore $1 + ap$ has order $p^{\ell-1}$. □

9.9 Theorem. *Let ℓ be a positive integer and let p be an odd prime. Then $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ is a cyclic group.*

PROOF: The cardinality of $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ is $\varphi(p^\ell) = p^{\ell-1}(p-1)$, so it suffices to find an integer of order $p^{\ell-1}(p-1)$ modulo p^ℓ. Let g be a primitive root modulo p. We have $g^{p-1} \equiv 1 \pmod{p}$, so either $g^{p-1} \equiv 1 + ap \pmod{p^2}$ for some a coprime with p, or $g^{p-1} \equiv 1 \pmod{p^2}$. In that latter case,

$$(g+p)^{p-1} = g^{p-1} + \frac{p-1}{1} g^{p-2} p + \cdots + p^{p-1}$$

so $(g+p)^{p-1} \equiv 1 + (p-1)g^{p-2}p \pmod{p^2}$. Note that $(p-1)g^{p-2}$ is copirme with p, so either g^{p-1} or $(g+p)^{p-1}$ is congruent to $1 + ap \pmod{p^2}$ with a coprime with p. Without lose of generality, we may suppose that $g^{p-1} \equiv 1 + ap \pmod{p^2}$. We claim that g generates $(\mathbb{Z}/p^\ell\mathbb{Z})^*$. Suppose that g has order m. Then $m \mid (p-1)p^{\ell-1}$, so $m = dp^s$ with $d \mid p-1$ and $0 \leq s \leq \ell - 1$. Thus $g^{dp^s} \equiv 1 \pmod{p^\ell}$, which implies that $g^{dp^s} \equiv 1 \pmod{p}$, so $g^d \equiv 1 \pmod{p}$ by Fermat's Little Theorem. Since g is a primitive root, $p - 1 \mid d$, so $d = p - 1$. Thus $m = (p-1)p^s$. But $g^{p-1} \equiv 1 + ap \pmod{p^2}$, thus $(g^{p-1})^{p^t} \equiv 1 + ap^{t+1} \pmod{p^{t+2}}$ by Proposition 9.8. Therefore $s = \ell - 1$ and the result follows. □

9.10 Theorem. *If $\ell \leq 2$ then $(\mathbb{Z}/2^\ell\mathbb{Z})^*$ is cyclic. If $\ell \geq 3$ then $(\mathbb{Z}/2^\ell\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\ell-2}\mathbb{Z}$. Finally, if $\ell \geq 3$ then $(\mathbb{Z}/2^\ell\mathbb{Z})^* = \{(-1)^a 5^b + 2^\ell\mathbb{Z} \mid 0 \leq a \leq 1, 0 \leq b < 2^{\ell-2}\}$.*

PROOF: Plainly, $(\mathbb{Z}/2\mathbb{Z})^*$ is cyclic if $\ell = 1$ or 2. Suppose that $\ell \geq 3$. We claim that for $\ell \geq 3$,

$$5^{2^{\ell-3}} \equiv 1 + 2^{\ell-1} \pmod{2^\ell}$$

The result holds for $\ell = 3$ by inspection. Suppose that the equation holds for some $\ell \geq 3$. Then there is an integer k so that $5^{2^{\ell-3}} = 1 + 2^{\ell-1} + k2^\ell$ Squaring both sides,

$$5^{2^{\ell-2}} = (1 + 2^{\ell-1} + k2^\ell)^2 = 1 + 2^\ell + k2^{\ell+1} + \cdots$$

Therefore $[5^{2^{\ell-2}} \equiv 1+2^\ell \pmod{2^{\ell+1}}$, and the claim follows by indution. It follows that the order of 5 in $(\mathbb{Z}/2^\ell\mathbb{Z})^*$ is $2^{\ell-2}$. Next we claim that the elements $(-1)^a 5^b$, with $0 \leq a \leq 1$, $0 \leq b < 2^{\ell-2}$ are all distinct modulo 2^ℓ. Suppose that $(-1)^{a_1}5^{b_1} \equiv (-1)^{a_2}5^{b_2} \pmod{2^\ell}$. Since $\ell \geq 3$, $(-1)^{a_1}5^{b_1} \equiv (-1)^{a_2}5^{b_2} \pmod 4$, so $(-1)^{a_1} \equiv (-1)^{a_2} \pmod 4$, so $a_1 = a_2$. It follows that $b_1 = b_2$ since $5^{b_1-b_2} \equiv 1 \pmod{2^\ell}$ and $|b_1 - b_2| < 2^{\ell-2}$. These $2^{\ell-1}$ elements are all distinct in $(\mathbb{Z}/2^\ell\mathbb{Z})^*$, which has order $2^{\ell-1}$. Therefore $(\mathbb{Z}/2^\ell\mathbb{Z})^* = \{(-1)^a 5^b + 2^\ell\mathbb{Z} \mid 0 \leq a \leq 1, 0 \leq b < 2^{\ell-2}\}$. It is now clear that $(\mathbb{Z}/2^\ell\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\ell-2}\mathbb{Z}$. □

9.11 Theorem. *The only positive integers m for which primitive roots exist modulo m are 1, 2, 4 and those integers off the form p^ℓ or $2p^\ell$, with p an odd prime and ℓ a postive integer.*

PROOF: Let $m > 1$ be an integer. Then let $m = 2^{\ell_0} p_1^{\ell_1} \cdots p_k^{\ell_k}$, where $\ell_i \geq 0$ and the p_i are odd primes. m has a primitive root if and only if $(\mathbb{Z}/m\mathbb{Z})^*$ is cyclic. By the Chinese Remainder Theorem,

$$(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/2^{\ell_0}\mathbb{Z})^* \times (\mathbb{Z}/p_1^{\ell_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k^{\ell_k}\mathbb{Z})^*$$

Now $(\mathbb{Z}/p_i^{\ell_i}\mathbb{Z})^*$ is cyclic of order $(p_i - 1)p_i^{\ell_i - 1}$ and $(\mathbb{Z}/2^{\ell_0}\mathbb{Z})^*$ is cyclic if $\ell_0 = 1$ or 2, and is ismorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\ell_0-2}\mathbb{Z}$ for $\ell_0 > 2$. Put $\lambda(m) = \operatorname{lcm}(b, \varphi(p_1^{\ell_1}), \ldots, \varphi(p_k^{\ell_k}))$, where $b = \varphi(2^{\ell_0})$ if $\ell_0 = 1$ or 2 and $b = \frac{\varphi(2^{\ell_0})}{2})$ if $\ell_0 > 2$. The order of an element of $(\mathbb{Z}/m\mathbb{Z})^*$ divides $\lambda(m)$. The order of $(\mathbb{Z}/m\mathbb{Z})^*$ is $\varphi(m)$. Since $2 \mid p_i - 1$, we see that $\lambda(m) < \varphi(m)$ whenever m is divisible by more than one odd prime or by a power of 2 larger than 4. Further, $\lambda(m) < \varphi(m)$ if $2^2 \mid m$ and m is divisible by an odd prime. The remaining cases are $m = 1$, 2, 4, p^ℓ, and $2p^\ell$. In each case the corresponding $(\mathbb{Z}/m\mathbb{Z})^*$ is cyclic. □

The function $\lambda(m)$ given in the proof is known as the *universal exponent* of m. The proof above gives us the proof of the following theorem as well. Note that since $\lambda(m) \mid \varphi(m)$, Theorem 9.12 is a strengthening of Euler's Theorem.

9.12 Theorem. *Let m be a positive integer and let a be coprime with m. Then $a^{\lambda(m)} \equiv 1 \pmod m$.*

Question: What is the smallest postive integer a such that a is a primitive root modulo p? Burgess proved that $a < c(\varepsilon)p^{\frac{1}{4}+\varepsilon}$, where $c(\varepsilon)$ is a positive number which depends on ε.

9.13 Theorem. *If p is a prime of the form $4q + 1$, where q is an odd prime, then 2 is a primitive root modulo p.*

PROOF: First notice that $p \equiv 5 \pmod 8$. Let t be the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^*$. Then $t \mid p - 1 = 4q$, so $t = 1$, 2, or 4, or q, $2q$, or $4q$. But $p = 13$ or $p \geq 29$, so $t \neq 1$, 2, or 4. It is enough to show that $2^{2q} \not\equiv 1 \pmod p$ to conclude that t has order $4q$ and hence that 2 is a primitive root modulo p. Note that

$$2^{2q} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod p$$

by Euler's Criterion. Since $p \equiv 5 \pmod 8$, $(\frac{2}{p}) = -1$ and the result follows. □

9.14 Theorem. *Let n be a positive integer. There are infinitely many primes p with $p \equiv 1 \pmod{n}$.*

Proof: Let $a > 2$ be an integer. We define the n^{th} cyclotomic polynomial by

$$\Phi_n(x) := \prod_{\substack{j=1\\(j,n)=1}}^{n} (x - \zeta_n^j)$$

where $\zeta_n = e^{\frac{2\pi i}{n}}$. Then $\Phi_n(x) \in \mathbb{Z}[x]$ and Φ_n has degree $\varphi(n)$. Further, $x^n - 1 = \prod_{d|n} \Phi_d(x)$. If p is a prime that divides $\Phi_n(a)$ then $p \equiv 1 \pmod{n}$ or $p \mid n$. To see this, note that if $p \mid \Phi_n(a)$ then $p \mid a^n - 1$. If $p \nmid a^d - 1$ for any proper divisor d of n then n is the order of a modulo p. Hence $n \mid p - 1$, so $p \equiv 1 \pmod{n}$. Suppose now that $p \mid a^d - 1$ for some proper divisor d of n. Since $p \mid \Phi_n(a)$, we see that $p \mid \frac{a^n-1}{a^d-1}$. Observe that

$$a^n = (1 + (a^d - 1))^{\frac{n}{d}} = 1 + \frac{n}{d}(a^d - 1) + \binom{\frac{n}{d}}{2}(a^d - 1)^2 + \cdots$$

so

$$\frac{a^n - 1}{a^d - 1} = \frac{n}{d} + \binom{\frac{n}{d}}{2}(a^d - 1) + + \binom{\frac{n}{d}}{3}(a^d - 1)^2 + \cdots$$

But this implies that $p \mid \frac{n}{d}$, so $p \mid n$.

Observe that if $p \mid \Phi_n(na)$ then $p \nmid n$, so $p \equiv 1 \pmod{n}$. Suppose there are only finitely many primes congruent to 1 modulo n, say $p_1, \dots, p_k$. Then $\Phi_n(np_1 \cdots p_k a)$ is only composed of primes congruent to 1 modulo n and is coprime with $p_1, \dots, p_k$. Thus $|\Phi_n(np_1 \cdots p_k a)| = 1$ for all a, which is a contradiction. □

9.1 Characters

In order to prove that for each pair of coprime integers a and b with $b > 0$ that there are infinitely many primes congruent to a modulo b we need to introduce characters.

9.15 Definition. Let G be a finite Abelian group. A *character* of G is a homomorphism $\chi : G \to \mathbb{C}^*$. The set of characters of G is called the *dual group* of G, denoted $\widehat{G}$.

The dual group truely is a group under pointwise multiplication. The identity element is the trivial homomorphism. Observe that $\chi(G) \subseteq \mathbb{T}$, and in fact $\chi(G)$ is a collection of $|G|^{\text{th}}$ roots of unity, since $\chi(g)^{|G|} = \chi(g^{|G|}) = \chi(1) = 1$, for all $g \in G$.

9.16 Theorem. *Let G be a finite Abelian group. Then*

1. $|G| = |\widehat{G}|$.
2. *G and $\widehat{G}$ are isomorphic.*
3. $\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = e \\ 0 & \text{otherwise} \end{cases}$
4. $\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = 1 \\ 0 & \text{otherwise} \end{cases}$

Proof: Recall that since G is a finite Abelian group it is a direct product of cyclic groups. In particular, there are elements $g_1, \dots, g_r \in G$ and positive integers $h_1, \dots, h_r$ such that every element $g \in G$ has a unique representation of the form $g = g_1^{t_1} \cdots g_r^{t_r}$, where $0 \le t_i < h_i$ for $i = 1, \dots, r$. Note that $|G| = h_1 \cdots h_r$. Here $g_1^0 \cdots g_r^0$ is the identity of the group and g_i has order h_i for $i = 1, \dots, r$. A character $\chi \in \widehat{G}$ is completely determined by its action on

g_i, for $i = 1, \dots, r$. But $(\chi(g_i))^{h_i} = \chi(g_i^{h_i}) = \chi(e) = 1$, so $\chi(g_i)$ is an h_i^{th} root of unity. Accordingly, there are at most $h_1 \cdots h_r$ different characters. But there are at least that many different characters since if ω_i is an h_i^{th} root of unity then the map $\chi(g) = \chi(g_1^{t_1} \cdots g_r^{t_r}) = (\chi(g_1))^{t_1} \cdots (\chi(g_r))^{t_r} = \omega_1^{t_1} \cdots \omega_r^{t_r}$ is a character of G. Thus $|G| = |\widehat{G}|$. Define $\varphi : G \to \widehat{G}$ by $\varphi(g) = \varphi(g_1^{t_1} \cdots g_r^{t_r}) = \chi_1^{t_1} \cdots \chi_r^{t_r}$, where $\chi_i : G \to \mathbb{C}^* : g_i \mapsto e^{\frac{2\pi i}{h_i}}$ and $\chi_i(g_j) = 1$ for $i \neq j$. Then φ is a group isomorphism.

Clear $\sum_{\chi \in \widehat{G}} \chi(e) = |\widehat{G}| = |G| = \sum_{g \in G} 1(g)$. Suppose that $g \neq e$. Then there is $\chi_1 \in \widehat{G}$ such that $\chi_1(g) \neq 1$. Futher, the map $\chi \mapsto \chi_1 \chi$ is a bijection. Therefore

$$\sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \chi_1(g)\chi(g) = \chi_1(g) \sum_{\chi \in \widehat{G}} \chi(g)$$

so $\sum_{\chi \in \widehat{G}} \chi(g) = 0$ since $\chi_1(g) \neq 1$. The proof for the last part is analogous. □

We shall be interested in characters associated with the group $(\mathbb{Z}/k\mathbb{Z})^*$, for $k \in \mathbb{N}$. Suppose that χ is a character of $(\mathbb{Z}/k\mathbb{Z})^*$. We associate to χ a map $\chi : \mathbb{Z} \to \mathbb{C}$, defined by

$$\chi(n) = \begin{cases} \chi([n]) & \text{if } \gcd(k,n) = 1 \\ 0 & \text{otherwise} \end{cases}$$

The map χ is known as a character modulo k. For any character χ of $(\mathbb{Z}/k\mathbb{Z})^*$, we can define the character $\overline{\chi}$ of $(\mathbb{Z}/k\mathbb{Z})^*$ by $\overline{\chi}([n]) = \overline{\chi([n])}$. Notice that $\chi\overline{\chi} = 1$, so $\overline{\chi}$ is the inverse of χ in the group $\widehat{(\mathbb{Z}/k\mathbb{Z})^*}$.

9.17 Theorem. *Let χ be a character modulo k.*

1. *If $\gcd(k,n) = 1$ then $\chi(n)$ is a $\varphi(k)^{th}$ root of unity.*
2. *$\chi(nm) = \chi(n)\chi(m)$ for all $n, m \in \mathbb{Z}$, so χ is completely multiplicative.*
3. *χ is periodic, with smallest period k.*
4. $\sum_{n=1}^{k} \chi(k) = \begin{cases} \varphi(k) & \textit{if } \chi = 1 \\ 0 & \textit{otherwise} \end{cases}$
5. $\sum_{\chi \in \widehat{\mathbb{Z}_k}} \chi(n) = \begin{cases} \varphi(k) & \textit{if } n \equiv 1 \pmod{k} \\ 0 & \textit{otherwise} \end{cases}$
6. *Let χ' be a character modulo k. Then* $\sum_{n=1}^{k} \chi'\chi(n) = \begin{cases} \varphi(k) & \textit{if } \chi' = \overline{\chi} \\ 0 & \textit{otherwise} \end{cases}$
7. $\sum_{\chi \in \widehat{\mathbb{Z}_k}} \overline{\chi}(m)\chi(n) = \begin{cases} \varphi(k) & \textit{if } m \equiv n \pmod{k} \textit{ and } \gcd(m,k) = 1 \\ 0 & \textit{otherwise} \end{cases}$

PROOF: Trivial, given Theorem 9.16. □

We have seen by the Chinese Remainder Theorem that the study of characters modulo k reduces to the study of characters modulo p^a for p prime and $a \in \mathbb{N}$. First suppose that p is odd. Let g be a primitive root modulo p^a. Suppose that $\gcd(n,p) = 1$. Then there is a unique integer $1 \leq \nu \leq \varphi(p^a)$ such that $g^\nu \equiv n \pmod{p^a}$. For each integer $1 \leq b \leq \varphi(p^a)$ we define the character

$$\chi^b(n) = \begin{cases} \exp\left(\frac{2\pi i \nu b}{\varphi(p^a)}\right) & \text{if } \gcd(b,p) = 1 \\ 0 & \text{otherwise} \end{cases}$$

We thus have $\varphi(p^a)$ such characters and so we have the complete collection. It remains to consider the characters modulo 2^a with $a \in \mathbb{N}$. If $a = 1$ then the only character is the principal character χ_0, where $\chi_0(n) = (n \mod 2)$. If $a = 2$ then we have the additional character

$$\chi_1(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \\ -1 & \text{if } n \equiv 3 \pmod 4 \\ 0 & \text{if } n \equiv 0 \pmod 2 \end{cases}$$

If $a \geq 3$ then $(\mathbb{Z}/2^a\mathbb{Z})^*$ is not cyclic. We've shown that if $n \equiv 1 \pmod 2$ then there are unique integers x and y such that $n \equiv (-1)^x 5^y \pmod{2^a}$ with $0 \leq x \leq 1$ and $0 \leq y < 2^{a-2}$. For each pair (b_1, b_2), with $0 \leq b_1 \leq 1$ and $0 \leq b_2 < 2^{a-2}$, we define the character

$$\chi_{(b_1,b_2)} = \begin{cases} \exp\left(\pi i x b_1 + \frac{\pi i y b_2}{2^{a-3}}\right) & \text{if } n \equiv 1 \pmod 2 \\ 0 & \text{if } n \equiv 0 \pmod 2 \end{cases}$$

This gives all of the $\varphi(2^a) = 2^{a-1}$ characters modulo 2^a. To get an explicit description of the group of characters modulo k for k composite, we just factor k into prime powers and take the product of the associated characters for each prime power.

9.18 Definition. Let $k \in \mathbb{N}$ and let χ be a character modulo k. We define the function $L(s,\chi)$ for $s \in \mathbb{C}$ with $\Re(s) > 1$ by

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

$L(s,\chi)$ is known as a *Dirichlet L function*.

The series $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ is uniformly convergent on compact subsets of $\Re(s) > 1$ and so it defines an analytic function for $\Re(s) > 1$. Since χ is completely multiplicative, $L(s,\chi)$ has an Euler product representation for $\Re(s) > 1$ given by

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

9.19 Theorem. *Let k be a postive integer and let χ be a character modulo k. The function $L(s,\chi)$ can be analytically continued to $\Re(s) > 0$, with the exception of the case where χ is the principal character, where there is a simple pole at $s = 1$ of residue $\frac{\varphi(k)}{k}$.*

PROOF: Let $A_\chi(x) = \sum_{n \leq x} \chi(n)$ and let $f(x) = \frac{1}{x^s}$. Note that

$$A_\chi(x) = \begin{cases} \varphi(k)\left[\frac{x}{k}\right] + R^0_{\chi_0}(x) & \text{if } \chi = \chi_0 \\ R_\chi(x) & \text{otherwise} \end{cases}$$

with $|R^0_{\chi_0}(x)| \leq \varphi(k)$ and $|R_\chi(x)| \leq \varphi(k)$ by Theorem 9.17. In the principal case, $A_{\chi_0}(x) = \varphi(k)\frac{x}{k} + R_{\chi_0}(x)$ with $|R_{\chi_0}(x)| \leq 2\varphi(k)$. By Abel summation,

$$\begin{aligned} \sum_{n \leq x} \frac{\chi_0(n)}{n^s} &= \frac{\varphi(k)}{k} x^{1-s} + \frac{R_{\chi_0}(x)}{x^s} + s\int_1^x \frac{A_{\chi_0}(u)}{u^{s+1}} du \\ &= \frac{\varphi(k)}{k} x^{1-s} + \frac{R_{\chi_0}(x)}{x^s} + s\frac{\varphi(k)}{k} \frac{u^{1-s}}{1-s}\Big]_1^x + s\int_1^x \frac{A_{\chi_0}(u)}{u^{s+1}} du \\ &= \frac{\varphi(k)}{k}\left(x^{1-s} + \frac{s}{s-1}x^{1-s} - \frac{s}{1-s}\right) + \frac{R_{\chi_0}(x)}{x^s} + s\int_1^x \frac{A_{\chi_0}(u)}{u^{s+1}} du \end{aligned}$$

If $\chi \neq \chi_0$ then again by Abel summation,

$$\sum_{n\le x}\frac{\chi(n)}{n^s}=\frac{R_\chi(x)}{x^s}+s\int_1^x\frac{R_\chi(u)}{u^{s+1}}du$$

Letting $x\to\infty$ we find that for $\Re(s)>1$,

$$\sum_{n=1}^{\infty}\frac{\chi_0(n)}{n^s}=\frac{\varphi(k)}{k}\frac{s}{s-1}+s\int_1^\infty\frac{R_{\chi_0}(u)}{u^{s+1}}du \qquad \text{and} \qquad \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}=s\int_1^\infty\frac{R_\chi(u)}{u^{s+1}}du$$

for $\chi \neq \chi_0$. Note that the right hand sides of both of these expressions converge to an analytic function for $\Re(s)>0$. The result follows. □

9.20 Definition. Let $(\lambda_n)_{n=1}^\infty$ be a strictly increasing sequence of positive real numbers. Let $(a_n)_{n=1}^\infty$ be a sequence of complex numbers. The *Dirichlet series* associated to $(\lambda_n)_{n=1}^\infty$ with coefficient sequence $(a_n)_{n=1}^\infty$ is the series $\sum_{n=1}^\infty a_n e^{-\lambda_n z}$ for $z\in\mathbb{C}$.

9.21 Theorem. *If the Dirichlet series $f(z)=\sum_{n=1}^\infty a_n e^{-\lambda_n z}$ converges at $z=z_0$ then it converges uniformly in the region $\Re(z-z_0)>0$ and $|\arg(z-z_0)|<\alpha$, for any $\alpha<2\pi$.*

Proof: By replacing z by $z-z_0$ and modifying the a_n's, we may assume without loss of generality that $z_0=0$. Therefore $\sum_{n=1}^\infty a_n$ converges. In particular, for each $\varepsilon>0$ there is $N=N(\varepsilon)$ such that if $\ell,m>N$ and we put $A_{\ell,m}=\sum_{n=\ell}^m a_n$ then $|A_{\ell,m}|<\varepsilon$. Observe that

$$\sum_{n=\ell}^{m}a_ne^{-\lambda_n z}=\sum_{n=\ell}^{m}(A_{\ell,n}-A_{\ell,n-1})e^{-\lambda_n z}=A_{\ell,m}e^{-\lambda_m z}+\sum_{n=\ell}^{m-1}A_{\ell,n}(e^{-\lambda_n z}-e^{-\lambda_{n+1}z})$$

Thus for $\ell,m>N$,

$$\left|\sum_{n=\ell}^{m}a_ne^{-\lambda_n z}\right|\le\varepsilon\left(|e^{-\lambda_m z}|+\sum_{n=\ell}^{m-1}|e^{-\lambda_n z}-e^{-\lambda_{n+1}z}|\right)$$

We may suppose that $\Re(z)>0$. Since $\lambda_m\in\mathbb{R}^+$ we see that $|e^{-\lambda_m z}|\le 1$. Further,

$$|e^{-\lambda_n z}-e^{-\lambda_{n+1}z}|=\left|z\int_{\lambda_n}^{\lambda_{n+1}}e^{-tz}dt\right|\le|z|\int_{\lambda_n}^{\lambda_{n+1}}e^{-tx}dt=|z|\left(-\frac{e^{-tx}}{x}\right]_{\lambda_n}^{\lambda_{n+1}}\right)\le\frac{|z|}{x}(e^{-\lambda_n x}-e^{-\lambda_{n+1}x})$$

where $z=x+iy$. Thus

$$\left|\sum_{n=\ell}^{m}a_ne^{-\lambda_n z}\right|\le\varepsilon\left(1+\frac{|z|}{x}\sum_{n=\ell}^{m-1}(e^{-\lambda_n x}-e^{-\lambda_{n+1}x})\right)=\varepsilon\left(1+\frac{|z|}{x}(e^{-\lambda_\ell x}-e^{-\lambda_m x})\right)\le 2\varepsilon\left(1+\frac{|z|}{x}\right)$$

If $\frac{|z|}{x}<k$ then the series converges uniformly. But $\frac{|z|}{x}<k$ implies that $|\arg(z)|<\alpha$ for some α depending upon k. The result now follows. □

If the Dirichlet series converges for $z=z_0$ then it converges uniformly on compact subsets of $\Re(z)>\Re(z_0)$ and so it defines an analytic funciton in this halfplane.

9.22 Theorem. *Let $f(z)=\sum_{n=1}^\infty a_n^{-\lambda_n z}$ be a Dirichlet series with $a_n\ge 0$ for all n. Let $\sigma_0\in\mathbb{R}$ and suppose that the series converges for $z=\sigma_0$. If f is analytic in a neighbourhood of σ_0 then there is $\varepsilon>0$ such that the series converges at $\sigma_0-\varepsilon$.*

Note by Theorem 9.21 that f converges for $\Re(z) > \sigma_0$, and we conclude that it converges for $\Re(z) > \sigma_0 - \varepsilon$.

PROOF: By translating by σ_0 we may assume without loss of generality that $\sigma_0 = 0$. Since f is analytic ina neighbourhood of 0 and by Theorem 9.21 is analytic for $\Re(z) > 0$, there is an $\varepsilon > 0$ such that f is a analytic in the disc $|z-1| \le 1+2\varepsilon$. Consider the Taylor expansion of f in this disc. For $\Re(z) > 0$,

$$f^{(m)}(z) = \sum_{n=1}^{\infty} (-\lambda_n)^m a_n e^{-\lambda_n z}$$

for $m \ge 0$. Hence $f^{(m)}(1) = \sum_{n=1}^{\infty} (-\lambda_n)^m a_n e^{-\lambda_n}$. The Taylor series of f around 1 on $|z-1| \le 1+2\varepsilon$ is given by

$$f(z) = \sum_{m=0}^{\infty} \frac{f^{(m)}(1)}{m!}(z-1)^m = \sum_{m=0}^{\infty}\sum_{n=1}^{\infty}(-\lambda_n)^m a_n e^{-\lambda_n}\frac{(z-1)^m}{m!}$$

Thus, if we take $z = -\varepsilon$ then

$$f(-\varepsilon) = \sum_{m=0}^{\infty}\sum_{n=1}^{\infty}\lambda_n^m a_n e^{-\lambda_n}\frac{(1+\varepsilon)^m}{m!}$$

Observe that since $a_n \ge 0$ we may change the order of summation. Thus

$$f(-\varepsilon) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n}\sum_{m=0}^{\infty}\lambda_n^m\frac{(1+\varepsilon)^m}{m!} = \sum_{n=1}^{\infty} a_n e^{-\lambda_n} e^{\lambda_n(1+\varepsilon)} = \sum_{n=1}^{\infty} a_n e^{-\lambda_n(-\varepsilon)}$$

So the series representation holds in this disc. □

If we have a Dirichlet series $\sum_{n=1}^{\infty} a_n e^{-\lambda_n z}$ defining a function $f(z)$ with $a_n \ge 0$ then the only obstruction to the series representing is a pole σ_1 of f on the real axis. The series will represent the function for all z with $\Re(z) > \sigma_1$.

9.23 Theorem. *Let k be a positive integer and let χ be a character modulo k. Then $L(s,\chi)$ is non-zero for $\Re(s) > 1$. Further, if χ is not the priniciple character then $L(1,\chi) \ne 0$.*

PROOF: $L(s,\chi)$ has a Euler product representation for $\Re(s) > 1$ given by $L(s,\chi) = \prod_p (1 - \frac{\chi(p)}{p^s})^{-1}$, and so is non-zero for $\Re(s) > 1$.

Suppose first that χ is a complex character. Then $\overline{\chi}$ is a character modulo k that is different from χ. From the Euler product, for any character χ modulo k, we have for $\Re(s) > 1$,

$$\log^* L(s,\chi) = \sum_p -\log\left(1 - \frac{\chi(p)}{p^s}\right)$$

where log denotes the principal branch of the logarithm and $\log^*$ denotes some branch of the logarithm. Then

$$\log^* L(s,\chi) = \sum_p \sum_{a=1}^{\infty} \frac{\chi(p)^a}{ap^{as}}$$

Let ℓ be an integer comprime with k. By Theorem 9.17

$$\sum_{\chi\in\widehat{\mathbb{Z}_k}} \overline{\chi}(\ell)\log^* L(s,\chi) = \sum_p\sum_{a=1}^{\infty}\sum_{\chi\in\widehat{\mathbb{Z}_k}}\frac{\overline{\chi}(\ell)\chi(p)^a}{ap^{as}} = \varphi(k)\sum_{\substack{p,a\\ p^a\equiv\ell\ (k)}}\frac{1}{ap^{as}} \tag{1}$$

In particular, we may take $\ell = 1$ in (1) and exponentiate to conclude that $\prod_{\chi \in \widehat{\mathbb{Z}_k}} L(s, \chi) \geq 1$, for $s \in \mathbb{R}$ and $s > 1$.

Suppose that χ is a non-prinicipal character modulo k. Then $\overline{\chi} \neq \chi$ if χ is not a real character. If $L(1, \chi) = 0$ then $L(1, \overline{\chi}) = \overline{L(1, \chi)} = 0$. Thus if χ is a complex character modulo k then there exist $c_1, c_2, c_3 > 0$ such that for $s \in \mathbb{R}$ with $1 < s \leq 2$, we have

$$|L(s, \chi_0)| \leq \frac{c_1}{s-1} \qquad L(s, \chi)L(s, \overline{\chi}) = |L(s, \chi)|^2 \leq c_s(s-1)^2 \qquad |L(s, \chi)| < c_3$$

for $\chi \neq \chi_0$. Thus, for $s \in \mathbb{R}$ with $1 < s \leq 2$,

$$1 \leq \left| \prod_{\chi \in \widehat{\mathbb{Z}_k}} L(s, \chi) \right| \leq \frac{c_1}{s-1} c_2 (s-1)^2 c_3 \leq c_1 c_2 c_3 (s-1)$$

Letting $s \to 1$ we obtain a contradiction. Therefore if χ is a complex character then $L(1, \chi) \neq 0$

Suppose now that χ is a real character with $\chi \neq \chi_0$. We introduce the function $g(s)$ defined for $\Re(s) > 1$ by $g(s) = \frac{\zeta(s)L(s,\chi)}{\zeta(2s)}$. By the Euler product representation for ζ and L, we see that for $\Re(s) > 1$,

$$\begin{aligned} g(s) &= \prod_p \frac{\left(1 - \frac{1}{p^{2s}}\right)}{\left(1 - \frac{1}{p^s}\right)\left(1 - \frac{\chi(p)}{p^s}\right)} \\ &= \prod_p \frac{1 + \frac{1}{p^s}}{1 - \frac{\chi(p)}{p^s}} \\ &= \prod_p \left(1 + \frac{1}{p^s}\right) \sum_{a=0}^{\infty} \frac{(\chi(p))^a}{p^{as}} \\ &= \prod_p \left(\sum_{a=0}^{\infty} \frac{\chi^a(p)}{p^{as}} \sum_{a=0}^{\infty} \frac{\chi^a(p)}{p^{(a+1)s}} \right) \\ &= \prod_p \left(1 + \sum_{a=1}^{\infty} \frac{\chi^a(p) + \chi^{a-1}(p)}{p^{as}} \right) \end{aligned}$$

Since χ is a real character, $b(a, p) := \chi^a(p) + \chi^{a-1}(p)$ is either 0 or 2. Accordingly, $g(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, where the a_n's are non-negative real numbers and where $a_1 = 1$. Recall that χ is non-principal, so $g(s)$ is analytic for $\Re(s) > 1$ and if $L(1, \chi) = 0$ then $\zeta(s)L(s, \chi)$ is analytic for $\Re(s) > 0$ since the simple pole of ζ at $s = 1$ is cancelled by the zero. Therefore if $L(1, \chi) = 0$ then $g(s)$ is anaytic for $\Re(s) > \frac{1}{2}$, since $\zeta(2s)$ is non-zero for $\Re(s) > \frac{1}{2}$. We now apply Theorems 9.21 and 9.22 to conclude that the series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges to $g(s)$ for $\Re(s) > \frac{1}{2}$. Since $\zeta(2s)$ has a simple pole at $s = \frac{1}{2}$, we see that $g(s)$ tends to 0 as s tends to $\frac{1}{2}$ from above on the real line. But $a_1 = 1$ and so $g(s)$ does not tend to 0 as s tends to $\frac{1}{2}$ from above. Therefore $L(1, \chi) \neq 0$. □

Proving that $L(1, \chi) \neq 0$ is what is needed to prove that whenever ℓ is an integer coprime with k that there are infinitely many primes p with $p \equiv \ell \pmod{k}$.

9.24 Theorem (Dirichlet's Theorem). *Let ℓ and k be coprime integers with $k \geq 2$. The series $\sum_{p \equiv \ell\ (k)} \frac{1}{p}$ is divergent, and so in particular, there are infinitely many primes p with $p \equiv \ell \pmod{k}$.*

Proof: Recall from the proof of Theorem 9.23, that

$$\frac{1}{\varphi(k)} \sum_{\chi \in \widehat{\mathbb{Z}_k}} \overline{\chi}(\ell) \log L(s, \chi) = \sum_{a=1}^{\infty} \sum_{p^a \equiv \ell\ (k)} \frac{1}{a p^{as}}$$

We now define $E(\chi)$ by

$$E(\chi) = \begin{cases} 1 & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise} \end{cases}$$

Note that as s tends to 1 from above on the real axis, $(s-1)^{E(\chi)}L(s,\chi)$ is bounded. Therefore, on the interval $(1,2)$, $E(\chi)\log(s-1) + \log L(s,\chi)$ is also bounded since $L(1,\chi) \neq 0$. Therefore there is a positive number c_1, which depends on k, such that

$$\left| \frac{1}{\varphi(k)} \sum_{\chi \in \widehat{\mathbb{Z}_k}} \overline{\chi}(\ell) \log L(s,\chi) + \frac{1}{\varphi(k)} \log(s-1) \right| < c_1$$

for $s \in (1,2)$. Accordingly,

$$\left| \sum_{a=1}^{\infty} \sum_{p^a \equiv \ell\ (k)} \frac{1}{ap^{as}} + \frac{1}{\varphi(k)} \log(s-1) \right| < c_1$$

for $s \in (1,2)$. We have

$$\sum_{a=1}^{\infty} \sum_{p^a \equiv \ell\ (k)} \frac{1}{ap^{as}} = \sum_{p \equiv \ell\ (k)} \frac{1}{p^s} + \sum_{a=2}^{\infty} \sum_{p^a \equiv \ell\ (k)} \frac{1}{ap^{as}}$$

Note that for $s \in (1,2)$

$$\begin{aligned} \sum_{a=2}^{\infty} \sum_{p^a \equiv \ell\ (k)} \frac{1}{ap^{as}} &\leq \sum_{a=2}^{\infty} \sum_{n=2}^{\infty} \frac{1}{an^{as}} \\ &\leq \sum_{a=2}^{\infty} \sum_{n=2}^{\infty} \frac{1}{2n^{as}} \\ &\leq \frac{1}{2} \sum_{n=2}^{\infty} \sum_{a=2}^{\infty} \frac{1}{n^{as}} \\ &\leq \frac{1}{2} \sum_{n=2}^{\infty} \sum_{a=2}^{\infty} \frac{1}{n^{2s}} \left(\frac{1}{1-\frac{1}{n}} \right) \\ &\leq \sum_{n=2}^{\infty} \frac{1}{n^2} < \frac{\pi^2}{6} \end{aligned}$$

Thus

$$\left| \sum_{p \equiv \ell\ (k)} \frac{1}{p^s} + \frac{1}{\varphi(k)} \log(s-1) \right| < c_1 + \frac{\pi^2}{6}$$

for $s \in (1,2)$. But as s tends to 1 from above on $(1,2)$ we see that $\frac{1}{\varphi(k)}\log(s-1)$ tends to $-\infty$. Therefore $\sum_{p \equiv \ell\ (k)} \frac{1}{p}$ diverges. □

Suppose that ℓ and k are coprime integers with $k \geq 2$. Let $\pi(x,k,\ell)$ denote the number of primes p with $p \leq x$ for which $p \equiv \ell \pmod{k}$. Then it can be proved that

$$\pi(x,k,\ell) \sim \frac{1}{\varphi(k)} \frac{x}{\log x} \sim \frac{1}{\varphi(k)} \mathrm{Li}(x)$$

Let H be a positive real number. It can be proved that if $k \leq (\log x)^H$ then

$$\pi(x,k,\ell) = \frac{\mathrm{Li}(x)}{\varphi(k)} + O(x \exp(-a\sqrt{\log x}))$$

for a a positive real number. On the other hand, with no constraint it can be shown that

$$\pi(x,k,\ell) = \frac{\mathrm{Li}}{\varphi(k)} + O(\frac{x}{(\log x)^H})$$

However, the big-O constants depend on H in an ineffective way. In other words, one cannot compute then in general.

Given ℓ_1 and ℓ_2 coprime with $k \geq 2$, with $\ell_1 \not\equiv \ell_2 \pmod{k}$, we have $\pi(x,k,\ell_1) \sim \pi(x,k,\ell_2)$. Chebyshev noted that for small x, $\pi(x,3,1) < \pi(x,3,2)$ and $\pi(x,4,1) < \pi(x,4,3)$. In 1957 Leech found the smallest x for which $\pi(x,4,1)$ exceeds $\pi(x,4,3)$, and it is 26 861. Bays and Hudson found the smallest x such that $\pi(x,3,1)$ exceeds $\pi(x,3,2)$, and it is 608 981 813 029.