PROBLEM SET # 2 SOLUTIONS

Chapter 2: Groups and Arithmetic

2.1 Groups.

1. Let G be a group and e and e' two identity elements. Show that $e = e'$. (*Hint*: Consider $e \cdot e'$ and calculate it two ways.)

   Solution. Since e is an identity element for G, we have $e \cdot g = g$ for every $g \in G$, and so in particular $e \cdot e' = e'$. On the other hand, since e' is an identity element for G, we also have $g \cdot e = g$ for every $g \in G$, and in particular $e \cdot e' = e$. Thus, $e' = e \cdot e' = e$. □

2. Let G be a group with identity e and such that $a^2 = e$ for every element a in G. Show that G is commutative, i.e., $a \cdot b = b \cdot a$ for every two elements a and b in G. (*Hint*: Consider $(a \cdot b)^2$.)

   Solution. First notice that, since $a^2 = e$ for every $a \in G$, we must have $a = a^{-1}$ for every $a \in G$. It then follows that $a \cdot b = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = b \cdot a$ for every pair of elements $a, b \in G$. □

9. Fix a positive integer n, and let $n\mathbf{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$ be the set of all integer multiples of n. Show that $n\mathbf{Z}$ is a subgroup of $\mathbf{Z}$ with respect to addition as binary operation.

   Solution. We need to check that $n\mathbf{Z}$ is closed under addition and inverse. So, suppose $a, b \in n\mathbf{Z}$, so that $a = jn$ and $b = kn$ for some integers $j, k \in \mathbf{Z}$. Then $a + b = jn + kn = (j + k)n \in n\mathbf{Z}$ and $-a = -(jn) = (-j)n \in n\mathbf{Z}$, and hence $n\mathbf{Z}$ is indeed closed under addition and inverse. □

2.2 Congruences.

1. Show that a positive integer m is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. (*Hint*: Notice that $10 \equiv -1 \mod 11$.)

   Solution. If $b_0, \ldots, b_k$ are the decimal digits of m (from the ones digit up to the 10^k-digit), then
   $$m = b_0 + b_1 \cdot 10 + \cdots + b_k \cdot 10^k.$$
   It follows that
   $$\begin{aligned} m &\equiv b_0 + b_1 \cdot (10) + \cdots + b_k \cdot (10)^k \mod 11 \\ &= b_0 + b_1 \cdot (-1) + \cdots + b_k \cdot (-1)^k \mod 11, \end{aligned}$$

and so m is congruent (modulo 11) to the alternating sum of its digits. Thus, m is divisible by 11 if and only if the alternating sum of its digits is. $\square$

2.3 Modular Arithmetic.

3. Write down the multiplication table for $\mathbf{Z}/11\mathbf{Z}$, the set of integers modulo 11. The subset of invertible integers modulo 11 is denoted by $(\mathbf{Z}/11\mathbf{Z})^\times$. Extract the multiplication table for $(\mathbf{Z}/11\mathbf{Z})^\times$.

   Solution. By a straightforward calculation, we find

$\cdot$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

From this table, we see that all of the nonzero elements of $\mathbf{Z}/11\mathbf{Z}$ are invertible, and the multiplication table for $(\mathbf{Z}/11\mathbf{Z})^\times$ is

$\cdot$	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

$\square$

4. Write down the multiplication table for $\mathbf{Z}/10\mathbf{Z}$, the set of integers modulo 10. The subset of invertible integers modulo 10 is denoted by $(\mathbf{Z}/10\mathbf{Z})^\times$. Extract the multiplication table for $(\mathbf{Z}/10\mathbf{Z})^\times$. How many invertible elements do we have here?

   Solution. By a straightforward calculation, we find

$\cdot$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	1	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

From this table, we see that the invertible elements of $\mathbf{Z}/10\mathbf{Z}$ are $1, 3, 7$, and 9, and the the multiplication table for $(\mathbf{Z}/10\mathbf{Z})^\times$ is

$\cdot$	**1**	**3**	**7**	**9**
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

□

5. Write down the multiplication table for $\mathbf{Z}/12\mathbf{Z}$, the set of integers modulo 12. The subset of invertible integers modulo 12 is denoted by $(\mathbf{Z}/12\mathbf{Z})^\times$. Extract the multiplication table for $(\mathbf{Z}/12\mathbf{Z})^\times$. How many invertible elements do we have here?

Solution. By a straightforward calculation, we find

$\cdot$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

From this table, we see that the invertible elements of $\mathbf{Z}/12\mathbf{Z}$ are $1, 5, 7$, and 11, and that the multiplication table for $(\mathbf{Z}/12\mathbf{Z})^\times$ is

$\cdot$	**1**	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

□

6. Use the Euclidean algorithm to compute the multiplicative inverse of 131 modulo 1979.

Solution. We first run the Euclidean algorithm:

$$\begin{aligned}1979 &= 15 \cdot 131 + 4\\ 131 &= 9 \cdot 14 + 5\\ 14 &= 2 \cdot 5 + 4\\ 5 &= 1 \cdot 4 + 1\\ 4 &= 4 \cdot 1.\end{aligned}$$

The second-to-last convergent in the continued fraction algorithm for $1979/131$ is therefore

$$15 + \cfrac{1}{9 + \frac{1}{2+\frac{1}{1}}} = \frac{423}{28}.$$

Observe, then, that $1979 \cdot 28 = 55412$ and $131 \cdot 423 = 55413$, and so $1979 \cdot (-28) + 131 \cdot (423) = 1$. Thus, the inverse of 131 modulo 1979 is 423. □

7. Use the Euclidean algorithm to compute the multiplicative inverse of 127 modulo 1091.

Solution. We first run the Euclidean algorithm:

$$\begin{aligned}1091 &= 8 \cdot 127 + 75\\ 127 &= 1 \cdot 75 + 52\\ 75 &= 1 \cdot 52 + 23\\ 52 &= 2 \cdot 23 + 6\\ 23 &= 3 \cdot 6 + 5\\ 6 &= 1 \cdot 5 + 1\\ 5 &= 5 \cdot 1.\end{aligned}$$

The second-to-last convergent in the continued fraction algorithm for $1091/127$ is therefore

$$8 + \cfrac{1}{1 + \frac{1}{1+\frac{1}{2+\frac{1}{3+\frac{1}{1}}}}} = \frac{189}{22}.$$

Observe, then, that $1091 \cdot 22 = 24002$ and $127 \cdot 189 = 24003$, and so $1091 \cdot (-22) + 127 \cdot (189) = 1$. Thus, the inverse of 127 modulo 1091 is 189. □

2.4 Theorem of Lagrange.

1. Let G be a group and g an element in G of order n. Let m be a positive integer such that $g^m = e$. Show that n divides m. (*Hint*: Write $m = qn + r$ with $0 \le r < n$.)

   Solution. Following the hint, we write $m = qn + r$ with $0 \le r < n$. Then observe that
   $$e = g^m = g^{qn+r} = (g^n)^q \cdot g^r = e^q \cdot g^r = g^r.$$
   Since $r < n$ and n is the order of g, we must therefore have $r = 0$. Thus $m = qn$, and hence n divides m. $\square$

2. Repeat the argument of Lagrange's theorem with $G = (\mathbf{Z}/13\mathbf{Z})^\times$ and $g = 5$.

   Solution. Following the proof, we first note that the order of $g = 5$ is 4. We then compute e, g, g^2, g^3. We obtain

e	g	g^2	g^3
1	5	12	8

   We see that $x = 2$ is missing from the list. We then compute x, xg, xg^2, xg^3, finding

x	xg	xg^2	xg^3
2	10	11	3

   We see that $y = 4$ has yet to appear in either of the above lists, so we next compute y, yg, yg^2, yg^4, finding

y	yg	yg^2	yg^3
4	7	9	6

   Looking over the three lists of numbers, we see that we have now accounted for every element of G exactly once, and that $12 = |G| = 3 \cdot 4 = 3 \cdot \mathrm{ord}(g)$, i.e., $\mathrm{org}(g)$ divides $|G|$. $\square$

2.5 Chinese Remainder Theorem.

2. Put $\phi(1) = 1$. Compute $\displaystyle\sum_{d|1000} \phi(d)$.

   Solution. Since $1000 = 2^3 \cdot 3^3$, the set of divisors of 1000 is $\{1, 2, 2\cdot 3, 2\cdot 3^2, 2\cdot 3^3, 2^2, 2^2\cdot 3, 2^2\cdot 3^2, 2^2\cdot 3^3, 2^3, 2^3\cdot 3, 2^3\cdot 3^2, 2^3\cdot 3^3\}$. We therefore have (using our known properties of ϕ)

$$\begin{aligned}
\sum_{d|1000} \phi(d) &= \phi(1) + \phi(2) + \cdots + \phi(2\cdot 3^3) + \phi(2^2) + \cdots + \phi(2^2\cdot 3^3) + \phi(2^3) + \cdots + \phi(2^3\cdot 3^3) \\
&= \left(\phi(1) + \phi(2) + \phi(2^2) + \phi(2^3)\right)\left(\phi(1) + \phi(3) + \phi(3^2) + \phi(3^3)\right) \\
&= \left(1 + (2-1) + (2^2-2) + (2^3-2^2)\right)\left(1 + (3-1) + (3^2-3) + (3^3-3^2)\right) \\
&= 2^3 \cdot 3^3 \\
&= 1000.
\end{aligned}$$

(Can you see how to prove the equality $\sum_{d|n} \phi(d) = n$ in general?) $\square$

3. Solve the system of congruences

$$x \equiv 5 \mod 11$$
$$x \equiv 7 \mod 13.$$

Solution. We follow the notation used in lecture. By a simple calculation, one can easily check that $y_1 = 6$ is the inverse of $M_1 = 13$ modulo $m_1 = 11$, and that $y_2 = 6$ is the inverse of $M_2 = 11$ modulo $m_2 = 13$. The solution to the system of equations is therefore

$$x \equiv 5 \cdot 13 \cdot 6 + 7 \cdot 11 \cdot 6 \mod (11 \cdot 13),$$

which simplifies to $x \equiv 137 \mod 143$. $\square$

4. Solve the system of congruences

$$x \equiv 11 \mod 16$$
$$x \equiv 16 \mod 27.$$

Solution. We follow the notation used in lecture. By a simple calculation, one can easily check that $y_1 = 3$ is the inverse of $M_1 = 27$ modulo $m_1 = 16$, and that $y_2 = 22$ is the inverse of $M_2 = 16$ modulo $m_2 = 27$. The solution to the system of equations is therefore

$$x \equiv 11 \cdot 27 \cdot 3 + 16 \cdot 16 \cdot 22 \mod (16 \cdot 27),$$

which simplifies to $x \equiv 43 \mod 432$. $\square$

5. Find the last two digits of 2^{9999}. Do not use a calculator.

Solution. Let $x = 2^{9999}$. We wish to compute the remainder of x modulo $100 = 4 \cdot 25$. We first observe that we obviously have $x = 2^{9999} \equiv 0 \mod 4$. Next observe that $2^{10} \equiv -1 \mod 25$, and so

$$\begin{aligned} x = 2^{9999} = (2^{10})^{999} \cdot 2^9 &\equiv (-1)^{999} \cdot (512) \mod 25 \\ &\equiv (-1) \cdot (12) \mod 25 \\ &\equiv 13 \mod 25. \end{aligned}$$

We now wish to solve the system of equation

$$x \equiv 0 \mod 4$$
$$x \equiv 13 \mod 25.$$

By a simple calculation, we see that $y_1 = 1$ is the inverse of $M_1 = 25$ modulo $m_1 = 4$, and $y_2 = 19$ is the inverse of $M_2 = 4$ modulo $m_2 = 25$. Thus, the solution to this system of equations is

$$x \equiv 0 \cdot 25 \cdot 1 + 13 \cdot 4 \cdot 19 \mod (4 \cdot 25),$$

which simplifies to $x \equiv 88 \mod 100$. Thus, the last two digits of $x = 2^{9999}$ are 88. $\square$