Practice Assignment 12

Chinese Remaindering and Algebraic Structures

Exercise 12–1

(a) Find x such that $3x \equiv 7 \mod 10$

(b) Find x such that $3x \equiv 6 \mod 12$

Solution:

(a) The inverse of 3 modulo 10 is $3^3 \equiv 27 \equiv 7 \pmod{10}$.
Hence, multiplying both sides of the above equation by 7, we obtain

$$\begin{aligned} 3x &\equiv 7 \pmod{10} \\ \Leftrightarrow 7 \cdot 3x &\equiv 7 \cdot 7 \pmod{10} \\ \Leftrightarrow x &\equiv 49 \equiv 9 \pmod{10} \end{aligned}$$

Hence, the solution is $x \equiv 9 \pmod{10}$.

(b) This time we don't have a multiplicative inverse to work with. So what to do?
Well, let's take a look at what this would mean. If $3x \equiv 6 \pmod{12}$, that means $3x - 6$ is divisible by 12, so there is some $k \in \mathbb{Z}$ such that $3x - 6 = 12k$. Now that we're working in the integers, we can happily divide by 3, and we thus obtain that $x - 2 = 4k$. Hence, we have that $x \equiv 2 \pmod 4$ solves the desired congruence.

Exercise 12–2

Find x, if possible, such that

(a) $2x \equiv 5 \mod 7$

$3x \equiv 4 \mod 8$

(b) $x \equiv 3 \mod 4$

$x \equiv 0 \mod 6$

Solution.

(a) First note that 2 has an inverse modulo 7, namely 4. So we can write the first equivalence as $x \equiv 4 \cdot 5 \equiv 6 \pmod 7$. Hence, we have that $x = 6 + 7k$ for some $k \in \mathbb{Z}$.
Now we can substitute this in for the second equivalence:

$$\begin{aligned} 3x &\equiv 4 \pmod 8 \\ 3(6 + 7k) &\equiv 4 \pmod 8 \\ 18 + 21k &\equiv 4 \pmod 8 \\ 2 + 5k &\equiv 4 \pmod 8 \\ 5k &\equiv 2 \pmod 8. \end{aligned}$$

Recalling that 5 has an inverse modulo 8, namely 5, we thus obtain

$$k \equiv 10 \equiv 2 \pmod 8.$$

Hence, we have that $k = 2 + 8j$ for some $j \in \mathbb{Z}$.
Plugging this back in for x, we have that $x = 6 + 7k = 6 + 7(2 + 8j) = 20 + 56j$ for some $j \in \mathbb{Z}$.
In fact, any choice of j will work here. Hence, we have that x is a solution to the system of congruences if and only if $x \equiv 20 \pmod{56}$.

(b) Let's work as we did above. From the first equivalence, we have that $x = 3 + 4k$ for some $k \in \mathbb{Z}$. Then, the second equivalence implies that $3 + 4k \equiv 0 \pmod{6}$, and hence $4k \equiv -3 \equiv 3 \pmod{6}$. However, this is impossible, since we know that $\gcd(4, 6) = 2$ and $2 \nmid 3$.

Exercise 12–3

Determine whether the following statements are true or false and justify your answer.

(a) There exists a finite field of order 243.

(b) There exists a finite field of order 8.

(c) There exists a finite field of order 12.

(d) There exists a finite field of order 500.

Solution:

(a) Yes, as $243 = 3^5$ and thus can be written as p^m.

(b) Yes, as $8 = 2^3$ and thus can be written as p^m.

(c) No, as $12 = 2^2 \times 3$

(d) No, as $500 = 2^2 \times 5^3$

Exercise 12–4

(a) Construct a table which describes the addition of all elements in the ring with each other for the ring Z_4.

(b) Construct the multiplication table for Z_4.

(c) Construct the addition and multiplication tables for Z_5.

(d) Construct the addition and multiplication tables for Z_6.

(e) There are elements in Z_4 and Z_6 without a multiplicative inverse. Which elements are these? Why does a multiplicative inverse exist for all non-zero elements in Z_5?

Solution:

(a) Multiplication Table for Z_4

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(b) Addition Table for Z_5

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication Table for Z_5

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1