Chapter 2

Congruence in $\mathbb{Z}$ and Modular Arithmetic

2.1 Congruence and Congruence Classes

1. (a) $2^{5-1} = 2^4 = 16 \equiv 1 \pmod 5$. (b) $4^{7-1} = 4^6 = 4096 \equiv 1 \pmod 7$.
   (c) $3^{11-1} = 3^{10} = 59049 \equiv 1 \pmod{11}$.

2. (a) Use Theorems 2.1 and 2.2: $6k + 5 \equiv 6.1 + 5 \equiv 11 \equiv 3 \pmod 4$.
   (b) $2r + 3s \equiv 2.3 + 3.(-7) \equiv -15 \equiv 5 \pmod{10}$.

3. (a) Computing the checksum gives

$$10 \cdot 3 + 9 \cdot 5 + 8 \cdot 4 + 7 \cdot 0 + 6 \cdot 9 + 5 \cdot 0 + 4 \cdot 5 + 3 \cdot 1 + 2 \cdot 8 + 1 \cdot 9$$
$$= 30 + 45 + 32 + 54 + 20 + 3 + 16 + 9 = 209.$$

   Since $209 = 11 \cdot 19$, we see that $209 \equiv 0 \pmod{11}$, so that this could be a valid ISBN number.

   (b) Computing the checksum gives

$$10 \cdot 0 + 9 \cdot 0 + 8 \cdot 3 + 7 \cdot 1 + 6 \cdot 1 + 5 \cdot 0 + 4 \cdot 5 + 3 \cdot 5 + 2 \cdot 9 + 1 \cdot 5$$
$$= 24 + 7 + 6 + 20 + 15 + 18 + 5 = 95.$$

   Since $95 = 11 \cdot 8 + 7$, we see that $95 \equiv 7 \pmod{11}$, so that this could not be a valid ISBN number.

   (c) Computing the checksum gives

$$10 \cdot 0 + 9 \cdot 3 + 8 \cdot 8 + 7 \cdot 5 + 6 \cdot 4 + 5 \cdot 9 + 4 \cdot 5 + 3 \cdot 9 + 2 \cdot 6 + 1 \cdot 10$$
$$= 27 + 64 + 35 + 24 + 45 + 20 + 27 + 12 + 10 = 264.$$

   Since $264 = 11 \cdot 24$, we see that $264 \equiv 0 \pmod{11}$, so that this could be a valid ISBN number.

4. (a) Computing the checksum gives

$$3 \cdot 0 + 3 + 3 \cdot 7 + 0 + 3 \cdot 0 + 0 + 3 \cdot 3 + 5 + 3 \cdot 6 + 6 + 3 \cdot 9 + 1 = 90.$$

Since $90 = 10 \cdot 9$, we have $90 \equiv 0 \pmod{10}$, so that this was scanned correctly.

(b) Computing the checksum gives

$$3 \cdot 8 + 3 + 3 \cdot 3 + 7 + 3 \cdot 3 + 2 + 3 \cdot 0 + 0 + 3 \cdot 0 + 6 + 3 \cdot 2 + 5 = 71.$$

Since $71 = 10 \cdot 7 + 1$, we have $71 \equiv 1 \pmod{10}$, so that this was not scanned correctly.

(c) Computing the checksum gives

$$3 \cdot 0 + 4 + 3 \cdot 0 + 2 + 3 \cdot 9 + 3 + 3 \cdot 6 + 7 + 3 \cdot 3 + 0 + 3 \cdot 3 + 4 = 83.$$

Since $83 = 10 \cdot 8 + 3$, we have $83 \equiv 3 \pmod{10}$, so that this was not scanned correctly.

5. Since $5 \equiv 1 \pmod 4$, it follows from Theorem 2.2 that $5^2 \equiv 1^2 \pmod 4$, so that (applying Theorem 2.2 again) $5^3 \equiv 1^3 \pmod 4$. Continuing, we get $5^{1000} \equiv 1^{1000} \equiv 1 \pmod 4$. Since $5^{1000} \equiv 1 \pmod 4$, Theorem 2.3 tells us that $\left[5^{1000}\right] = [1]$ in $\mathbb{Z}_4$.

6. Given $n \mid (a - b)$ so that $a - b = nq$ for some integer q. Since $k \mid n$ it follows that $k \mid (a - b)$ and therefore $a \equiv b \pmod k$.

7. By Corollary 2.5, $a \equiv 0, 1, 2$ or $3 \pmod 4$. Theorem 2.2 implies $a^2 \equiv 0, 1 \pmod 4$. Therefore a^2 cannot be congruent to either 2 or 3 (mod 4).

8. By the division algorithm, any integer n is expressible as $n = 4q + r$ where $r \in \{0, 1, 2, 3\}$, and $n \equiv r \pmod 4$. If r is 0 or 2 then n is even. Therefore if n is odd then $n \equiv 1$ or $3 \pmod 4$.

9. (a) $(n - a)^2 \equiv n^2 - 2na + a^2 \equiv a^2 \pmod n$ since $n \equiv 0 \pmod n$.
(b) $(2n - a)^2 \equiv 4n^2 - 4na + a^2 \equiv a^2 \pmod{4n}$ since $4n \equiv 0 \pmod{4n}$.

10. Suppose the base ten digits of a are $(c_n c_{n-1} \ldots c_1 c_0)$. (Compare Exercise 1.2.32). Then $a = c_n 10^n + c_{n-1} 10^{n-1} + \ldots c_1 10 + c_0 \equiv c_0 \pmod{10}$, since $10^k \equiv 0 \pmod{10}$ for every $k \geq 1$.

11. Since there are infinitely many primes (Exercise 1.3.25) there exists a prime $p > |a - b|$. By hypothesis, $p \mid (a - b)$ so the only possibility is $a - b = 0$ and $a = b$.

12. If $p \equiv 0, 2$ or $4 \pmod 6$, then p is divisible by 2. If $p \equiv 0$ or $3 \pmod 6$ then p is divisible by 3. Since p is a prime > 3 these cases cannot occur, so that $p \equiv 1$ or $5 \pmod 6$. By Theorem 2.3 this says that $[p] = [1]$ or $[5]$ in $\mathbb{Z}_6$.

13. Suppose r, r' are the remainders for a and b, respectively. Theorem 2.3 and Corollary 2.5 imply: $a \equiv b \pmod n$ if and only if $[a] = [b]$ if and only if $[r] = [r']$. Then $r = r'$ as in the proof of Corollary 2.5(2).

14. (a) Here is one example: $a = b = 2$ and $n = 4$.
    (b) The assertion is: if $n \mid ab$ then either $n \mid a$ or $n \mid b$. This is true when n is prime by Theorem 1.8.

15. Since $(a, n) = 1$ there exist integers u, v such that $au + nv = 1$, by Theorem 1.3. Therefore $au \equiv au + nv \equiv 1 \pmod{n}$, and we can choose $b = u$.

16. Given that $a \equiv 1 \pmod{n}$, we have $a = nq + 1$ for some integer q. Then (a, n) must divide $a - nq = 1$, so $(a, n) = 1$. One example to see that the converse is false is to use $a = 2$ and $n = 3$. Then $(a, n) = 1$ but $[a] \neq [1]$.

17. Since $10 \equiv -1 \pmod{11}$, Theorem 2.2 (repeated) shows that $10^n \equiv (-1)^n \pmod{11}$.

18. By Exercise 23 we have $125698 \equiv 31 \equiv 4 \pmod{9}$, $23797 \equiv 28 \equiv 1 \pmod{9}$ and $2891235306 \equiv 39 \equiv 12 \equiv 3 \pmod{9}$. Since $4 \cdot 1 \not\equiv 3 \pmod{9}$ the conclusion follows.

19. Proof: If $[a] = [b]$ then $a \equiv b \pmod{n}$ so that $a = b + nk$ for some integer k. Then $(a, n) = (b, n)$ using Lemma 1.7.

20. (a) One counterexample occurs when $a = 0$, $b = 2$ and $n = 4$.
    (b) Given $a^2 \equiv b^2 \pmod{n}$, we have $n \mid (a^2 - b^2) = (a + b)(a - b)$. Since n is prime, use Theorem 1.8 to conclude that either $n \mid (a + b)$ or $n \mid (a - b)$. Therefore, either $a \equiv b \pmod{n}$ or $a \equiv -b \pmod{n}$.

21. (a) Since $10 \equiv 1 \pmod{9}$, Theorem 2.2 (repeated) shows that $10^n \equiv 1 \pmod{9}$.
    (b) (Compare Exercise 1.2.32). Express integer a in base ten notation: $a = c_n 10^n + \ldots + c_1 10 + c_0$. Then $a \equiv c_n + c_{n-t} + \ldots c_1 + c_0 \pmod{9}$, since $10^k \equiv 1 \pmod{9}$.

22. (a) Here is one example: $a = 2$, $b = 0$, $c = 2$, $n = 4$.
    (b) We have $n \mid ab - ac = a(b - c)$. Since $(a, n) = 1$ Theorem 1.5 implies that $n \mid (b - c)$ and therefore $b \equiv c \pmod{n}$.

2.2 Modular Arithmetic

1. (a) Answered in the text.

   (b)

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

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

(c) Answered in the text.

(d)

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

	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

However, the notation must be changed to correspond to the new notation. See the tables in Example 2 to see what it must look like.

2. To solve $x^2 \oplus x = [0]$ in $\mathbb{Z}_4$, substitute each of $[0], [1], [2]$, and $[3]$ in the equation to see if it is a solution:

x	$x^2 \oplus x$	Is $x^2 \oplus x = [0]$?
$[0]$	$[0] \otimes [0] \oplus [0] = [0] + [0] = [0]$	Yes; solution.
$[1]$	$[1] \otimes [1] \oplus [1] = [1] + [1] = [2]$	No.
$[2]$	$[2] \otimes [2] \oplus [2] = [0] + [2] = [2]$	No.
$[3]$	$[3] \otimes [3] \oplus [3] = [1] \oplus [3] = [0]$	Yes; solution.

3. $x = 1, 3, 5$ or 7 in $\mathbb{Z}_0$. However, the notation should be changed to use, for example, $[3]$ instead of 3.

4. $x = 1, 2, 3$ or 4 in $\mathbb{Z}_5$. However, the notation should be changed to use, for example, [3] instead of 3.

5. $x = 1, 2, 4, 5$ in $\mathbb{Z}_6$. However, the notation should be changed to use, for example, [3] instead of 3.

6. To solve $x^2 \oplus [8] \otimes x = [0]$ in $\mathbb{Z}_9$, substitute each of $[0], [1], [2], \ldots, [8]$ in the equation to see if it is a solution:

x	$x^2 \oplus [8] \otimes x$	Is $x^2 \oplus [8] \otimes x = [0]$?
$[0]$	$[0] \otimes [0] \oplus [8] \otimes [0] = [0] + [0] = [0]$	Yes; solution.
$[1]$	$[1] \otimes [1] \oplus [8] \otimes [1] = [1] + [8] = [0]$	Yes; solution.
$[2]$	$[2] \otimes [2] \oplus [8] \otimes [2] = [4] + [7] = [2]$	No.
$[3]$	$[3] \otimes [3] \oplus [8] \otimes [3] = [0] \oplus [6] = [6]$	No.
$[4]$	$[4] \otimes [4] \oplus [8] \otimes [4] = [7] \oplus [5] = [3]$	No.
$[5]$	$[5] \otimes [5] \oplus [8] \otimes [5] = [7] \oplus [4] = [2]$	No.
$[6]$	$[6] \otimes [6] \oplus [8] \otimes [6] = [0] \oplus [3] = [3]$	No.
$[7]$	$[7] \otimes [7] \oplus [8] \otimes [7] = [4] \oplus [2] = [6]$	No.
$[8]$	$[8] \otimes [8] \oplus [8] \otimes [8] = [1] \oplus [1] = [2]$	No.

The solutions are $x = [0]$ and $x = [1]$.

7. To solve $x^3 \oplus x^2 \oplus x \oplus [1] = [0]$ in $\mathbb{Z}_8$, substitute each of $[0], [1], [2], \ldots, [7]$ in the equation to see if it is a solution:

x	$x^3 \oplus x^2 \oplus x \oplus [1]$	Is $x^3 \oplus x^2 \oplus x \oplus [1] = [0]$?
$[0]$	$[1]$	No.
$[1]$	$[4]$	No.
$[2]$	$[7]$	No.
$[3]$	$[0]$	No.
$[4]$	$[5]$	No.
$[5]$	$[4]$	No.
$[6]$	$[3]$	No.
$[7]$	$[0]$	Yes; solution.

The only solution is $x = [7]$.

8. To solve $x^3 + x^2 = [2]$ in $\mathbb{Z}_{10}$, substitute each of $[0], [1], \ldots, [9]$ in the equation to see if it is a

solution:

x	$x^3 \oplus x^2$	Is $x^3 \oplus x^2 = [2]$?
[0]	[0]	No.
[1]	[2]	Yes; solution.
[2]	[2]	Yes; solution..
[3]	[6]	No.
[4]	[0]	No.
[5]	[0]	No.
[6]	[2]	Yes; solution.
[7]	[2]	Yes; solution.
[8]	[6]	No.
[9]	[0]	No.

The solutions are $x = [1], [2], [6]$, and $[7]$.

9. (a) $a = 3$ or 5. (b) $a = 2$ or 3. (c) No such element exists in $\mathbb{Z}_6$.
   However, the notation should be changed to use, for example, [3] instead of 3.

10. Part 3: $[a] \oplus [b] = [a + b] = [b + a] = [b] \oplus [a]$ since $a + b = b + a$ in $\mathbb{Z}$.

    Part 7: $[a] \odot ([b] \odot [c]) = [a] \odot [be] = [a(bc)] = [(ab)c] = [ab] \odot [c] = ([a] \odot [b]) \odot [c]$.

    Part 8: $[a] \odot ([b] \oplus [c]) = [a] \odot [b + c] = [a(b + c)] = [ab + ac] = [ab] \oplus [ac] = ([a] \odot [b]) \oplus ([a] \odot [c])$.

    Part 9: $[a] \odot [b] = [ab] = [ba] = [b] \odot [a]$.

11. Every value of x satisfies these equations.

12. See Exercise 2.1.14.

13. See Exercise 2.1.22.

14. (a) $x = 0$ or 4 in $\mathbb{Z}_5$. (b) $x = 0, 2, 3$ or 5 in $\mathbb{Z}_6$.
    However, the notation should be changed to use, for example, [3] instead of 3.

15. (a) $(a+b)^5 = a^5 + b^5$ in $\mathbb{Z}_5$. (b) $(a+b)^3 = a^3 + b^3$ in $\mathbb{Z}_3$.

(c) $(a+b)^2 = a^2 + b^2$ in $\mathbb{Z}_2$.

(d) One is led to conjecture that $(a+b)^7 = a^7 + b^7$ in $\mathbb{Z}_7$.

To investigate the general result for any prime exponent, use the Binomial Theorem and Exercise 1.4.13.

However, the notation should be changed to use, for example, $[a]$ instead of a.

16. (a) $a = 1, 2, 3$ or 4 in $\mathbb{Z}_5$. (b) $a = 1$ or 3 in $\mathbb{Z}_4$.

(c) $a = 1$ or 2 in $\mathbb{Z}_3$ (d) a = 1 or 5 in $\mathbb{Z}_6$.

However, the notation should be changed to use, for example, $[3]$ instead of 3.

2.3 The Structure of $\mathbb{Z}_p$ (p Prime) and $\mathbb{Z}_n$

1. (a) 1, 2, 3, 4, 5, 6 (b) 1, 3, 5, 7

(c) 1, 2, 4, 5, 7, 8 (d) 1, 3, 7, 9

2. (a) Since 7 is prime, part (3) of Theorem 2.8 says that there are no zero divisors in $\mathbb{Z}_7$.
   (b) The zero divisors are 2, 4, and 6, since $2 \cdot 4 = 0$ and $6 \cdot 4 = 0$. Further computations will show that the other elements of $\mathbb{Z}_8$ are not zero divisors.
   (c) The zero divisors are 3 and 6, since $3 \cdot 6 = 0$. Further computations will show that the other elements of $\mathbb{Z}_9$ are not zero divisors.
   (d) The zero divisors are $2, 4, 5, 6$, and 8, since $2 \cdot 5 = 4 \cdot 5 = 6 \cdot 5 = 8 \cdot 5 = 0$. Further computations will show that the other elements of $\mathbb{Z}_{10}$ are not zero divisors.

3. In $\mathbb{Z}_n$, it appears that every nonzero element is either a unit or a zero divisor.

4. (a) 1 solution in $\mathbb{Z}_7$ (b) 2 solutions in $\mathbb{Z}_8$

(c) 0 solutions in $\mathbb{Z}_9$ (d) 2 solutions in $\mathbb{Z}_{10}$.

5. We first show that $ab \neq 0$. If $ab = 0$, then since a is a unit, then $a^{-1}ab = 0$, so that $b = 0$. But b is a zero divisor, so that $b \neq 0$ and thus $ab \neq 0$. Now, since b is a zero divisor, choose $c \neq 0$ such that $bc = 0$; then $(ab)c = a(bc) = 0$ shows that ab is also a zero divisor.

6. Since n is composite, write $n = ab$ where $1 < a, b < n$. Then in $\mathbb{Z}_n$, $[a] \neq 0$ and $[b] \neq 0$, since both a and b are less than n, but $[a][b] = [ab] = [n] = 0$, so that a and b are zero divisors.

7. If $ab = 0$ in $\mathbb{Z}_p$ then $ab \equiv 0 \pmod{p}$ so that $p \mid ab$. By Theorem 1.8 we conclude that $p \mid a$ or $p \mid b$. Then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$. Equivalently, $a = 0$ or $b = 0$ in $\mathbb{Z}_p$.

8. (a) For instance choose a even and b odd. (b) Yes.

9. (a) Suppose a is a unit. Choose b such that $ab = 0$. Then since a is a unit, we have $a^{-1}ab = a^{-1}0 = 0$, so that $b = 0$. Thus a is not a zero divisor, since any such b must be zero.
   (b) This statement is the contrapositive of part (a), so is also true.

10. No element can be both a unit and a zero divisor, by Exercise 9. Choose $x \neq 0 \in \mathbb{Z}_n$, and consider the set of products $\{x \cdot 1, x \cdot 2, \ldots, x \cdot (n-1)\}$. This set has $n-1$ elements. If x is not a zero divisor, then 0 is not one of those elements. So there are two possibilities: either no element is duplicated in that list, or there is a duplicate. If there is no duplicate, then since there are $n-1$ elements and $n-1$ possible values, one of the elements must be 1; that is, for some $a \in \mathbb{Z}_n$, we have $x \cdot a = 1$. Thus x is a unit. If there is a duplicate, say $x \cdot a = x \cdot b$, then $x \cdot (a-b) = 0$, so that x is a zero divisor, which contradicts our original assumption. This shows that if x is not a zero divisor, then it is a unit.

11. Since a is a unit, the equation $ax = b$ has the solution $a^{-1}b$, since $aa^{-1}b = b$. Now, suppose that $ax = b$ and also $ay = b$. Then $a(x-y) = 0$. Since a is not a zero divisor, and $a \neq 0$ since it is a unit, it follows that $x - y = 0$ so that $x = y$. Hence the solution is unique.

12. If $x = [r]$ is a solution then $[ar] = [b]$ so that $ar \equiv b \pmod n$ and $ar - b = kn$ for some integer k. Then $d \mid a$ and $d \mid n$ implies $d \mid (ar - kn) = b$.

13. Since d divides each of a, b and n there are integers a_1, n_1, b_1. with $a = da_1$, $b = db_1$. and $n = dn_1$. By Theorem 1.3 there are integers u, v with $au + nv = d$ so that $au \equiv d \pmod n$. Therefore $a(ub_1) \equiv b_1 d = b \pmod n$ so that $x = [ub_1]$ is one solution. Since $an_1 = a_1 dn_1 = a_1 n \equiv 0 \pmod n$ we see that $x = [ub_1 + n_1 t]$ is a solution for every integer t.

14. (a) If $[ub_1 + sn_1]$ and $[ub_1 + tn_1]$ are equal in $\mathbb{Z}_n$ for some $0 \leq s < t < d$, then $n \mid (tn_1 - sn_1) = (t-s)n_1$ so that $d \mid (t-s)$ contrary to $0 < (t-s) < d$.
    (b) If $x = [r]$ is a solution then $[ar] = [b] = [a \cdot ub_1]$ so that $n \mid a(r - ub_1)$ so that $a(r - ub_1) = nw$ for some integer w. Cancel d to obtain $a_1(r - ub_1) = n_1 w$. Since $(a_1, n_1) = 1$, (Why?) Theorem 1.5 implies $n_1 \mid (r - ub_1)$ so that $r = ub_1 + tn_1$ for some t. Then $x = [r] = [ub_1 + tn_1]$. Divide t by d to get $t = dq + k$ where $0 \leq k < d$. Then $x = [ub_1 + (dq + k)n_1] = [ub_1 + kn_1]$ because $[dn_1] = [n] = [0]$.

15. (a) $15x = 9$ in Z_{18} if and only if $15x \equiv 9 \pmod{18}$ if and only if $5x \equiv 3 \pmod 6$ if and only if $x \equiv 3 \pmod 6$ if and only if $x \equiv 3, 9, 15 \pmod{18}$ if and only if $x = [3], [9], [15]$ in Z_{18}.
    (b) $x = 3, 16, 29, 42$ or 55 in Z_{65}.

16. By Exercise 10, every nonzero element of $\mathbb{Z}_n$ is a unit or a zero divisor, but not both. So the statement we are trying to prove is equivalent to the following statement: If $a \neq 0$ and b are elements of $\mathbb{Z}_n$ and $ax = b$ has no solutions in $\mathbb{Z}_n$, prove that a is not a unit. The contrapositive of this statement, which is equivalent to the statement itself, is: If $a \neq 0$ and b are elements of $\mathbb{Z}_n$ and a is a unit, then $ax = b$ has at least one solution in $\mathbb{Z}_n$. But Exercise 11 proves this statement.

17. Suppose that a and b are units. Then $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$, so that ab is a unit.

18. See the Hint when $0 < 1$. Otherwise, if $0 \not< 1$, then since $0 = 1$, we must have $1 < 0$ since we have fully ordered $\mathbb{Z}_n$. Adding 1 to both sides repeatedly, using rule (ii), gives $n-1 < n-2 < \cdots < 1 < 0$, so that, by rule (i), $n - 1 < 0$. Now add 1 to both sides to get $0 < 1$, which is a contradiction.