Chapter 1

Arithmetic in $\mathbb{Z}$ Revisited

1.1 The Division Algorithm

1. (a) $q = 4$, $r = 1$. (b) $q = 0$, $r = 0$. (c) $q = -5$, $r = 3$.

2. (a) $q = -9$, $r = 3$. (b) $q = 15$, $r = 17$. (c) $q = 117$, $r = 11$.

3. (a) $q = 6$, $r = 19$. (b) $q = -9$, $r = 54$. (c) $q = 62720$, $r = 92$.

4. (a) $q = 15021$, $r = 132$. (b) $q = -14940$, $r = 335$. (c) $q = 39763$, $r = 3997$.

5. Suppose $a = bq + r$, with $0 \le r < b$. Multiplying this equation through by c gives $ac = (bc)q + rc$. Further, since $0 \le r < b$, it follows that $0 \le rc < bc$. Thus this equation expresses ac as a multiple of bc plus a remainder between 0 and $bc - 1$. Since by Theorem 1.1 this representation is unique, it must be that q is the quotient and rc the remainder on dividing ac by bc.

6. When q is divided by c, the quotient is k, so that $q = ck$. Thus $a = bq + r = b(ck) + r = (bc)k + r$. Further, since $0 \le r < b$, it follows (since $c \ge 1$) than $0 \le r < bc$. Thus $a = (bc)k + r$ is the unique representation with $0 \le r < bc$, so that the quotient is indeed k.

7. Answered in the text.

8. Any integer n can be divided by 4 with remainder r equal to 0, 1, 2 or 3. Then either $n = 4k$, $4k + 1$, $4k + 2$ or $4k + 3$, where k is the quotient. If $n = 4k$ or $4k + 2$ then n is even. Therefore if n is odd then $n = 4k + 1$ or $4k + 3$.

9. We know that every integer a is of the form $3q$, $3q + 1$ or $3q + 2$ for some q. In the last case $a^3 = (3q + 2)^3 = 27q^3 + 54q^2 + 36q + 8 = 9k + 8$ where $k = 3q^3 + 6q^2 + 4q$. Other cases are similar.

10. Suppose $a = nq + r$ where $0 \le r < n$ and $c = nq' + r'$ where $0 < r' < n$. If $r = r'$ then $a - c = n(q - q')$ and $k = q - q'$ is an integer. Conversely, given $a - c = nk$ we can substitute to find: $(r - r') = n(k - q + q')$. Suppose $r \ge r'$ (the other case is similar). The given inequalities imply that $0 \le (r - r') < n$ and it follows that $0 \le (k - q + q') < 0$ and we conclude that $k - q + q' = 0$. Therefore $r - r' = 0$, so that $r = r'$ as claimed.

11. Given integers a and c with $c \neq 0$. Apply Theorem 1.1 with $b = |c|$ to get $a = |c| \cdot q_0 + r$ where $0 \leq r < |c|$. Let $q = q_0$ if $c > 0$ and $q = -q_0$ if $c < 0$. Then $a = cq + r$ as claimed. The uniqueness is proved as in Theorem 1.1.

1.2 Divisibility

1. (a) 8. (b) 6. (c) 1. (d) 11. (e) 9. (f) 17. (g) 592. (h) 6.

2. If $b \mid a$ then $a = bx$ for some integer x. Then $a = (-b)(-x)$ so that $(-b) \mid a$. The converse follows similarly.

3. Answered in the text.

4. (a) Given $b = ax$ and $c = ay$ for some integers x, y, we find $b + c = ax + ay = a(x + y)$. Since $x + y$ is an integer, conclude that $a \mid (b + c)$.
   (b) Given x and y as above we find $br + ct = (ax)r + (ay)t = a(xr + yt)$ using the associative and distributive laws. Since $xr + yt$ is an integer we conclude that $a \mid (br + ct)$.

5. Since $a \mid b$, we have $b = ak$ for some integer k, and $a \neq 0$. Since $b \mid a$, we have $a = bl$ for some integer l, and $b \neq 0$. Thus $a = bl = (ak)l = a(kl)$. Since $a \neq 0$, divide through by a to get $1 = kl$. But this means that $k = \pm 1$ and $l = \pm 1$, so that $a = \pm\, b$.

6. Given $b = ax$ and $d = cy$ for some integers x, y, we have $bd = (ax)(cy) = (ac)(xy)$. Then $ac \mid bd$ because xy is an integer.

7. Clearly $(a, 0)$ is at most $|a|$ since no integer larger than $|a|$ divides a. But also $|a| \mid a$, and $|a| \mid 0$ since any nonzero integer divides 0. Hence $|a|$ is the gcd of a and 0.

8. If $d = (n, n + 1)$ then $d \mid n$ and $d \mid (n + 1)$. Since $(n + 1) - n = 1$ we conclude that $d \mid 1$. (Apply Exercise 4(b).) This implies $d = 1$, since $d > 0$.

9. No, ab need not divide c. For one example, note that $4 \mid 12$ and $6 \mid 12$, but $4 \cdot 6 = 24$ does not divide 12.

10. Since $a \mid a$ and $a \mid 0$ we have $a \mid (a, 0)$. If $(a, 0) = 1$ then $a \mid 1$ forcing $a = \pm 1$.

11. (a) 1 or 2 (b) 1, 2, 3 or 6. Generally if $d = (n, n + c)$ then $d \mid n$ and $d \mid (n + c)$. Since c is a linear combination of n and n+c, conclude that $d \mid c$.

12. (a) False. (ab, a) is always at least a since $a \mid ab$ and $a \mid a$.
    (b) False. For example, $(2, 3) = 1$ and $(2, 9) = 1$, but $(3, 9) = 3$.
    (c) False. For example, let $a = 2$, $b = 3$, and $c = 9$. Then $(2, 3) = 1 = (2, 9)$, but $(2 \cdot 3, 9) = 3$.

13. (a) Suppose $c \mid a$ and $c \mid b$. Write $a = ck$ and $b = cl$. Then $a = bq + r$ can be rewritten $ck = (cl)q + r$, so that $r = ck - clq = c(k - lq)$. Thus $c \mid r$ as well, so that c is a common divisor of b and r.

(b) Suppose $c \mid b$ and $c \mid r$. Write $b = ck$ and $r = cl$, and substitute into $a = bq + r$ to get $a = ckq + cl = c(kq + l)$. Thus $c \mid a$, so that c is a common divisor of a and b.

(c) Since (a, b) is a common divisor of a and b, it is also a common divisor of b and r, by part (a). If (a, b) is not the greatest common divisor (b, r) of b and r, then $(a, b) > (b, r)$. Now, consider (b, r). By part (b), this is also a common divisor of (a, b), but it is less than (a, b). This is a contradiction. Thus $(a, b) = (b, r)$.

14. By Theorem 1.3, the smallest positive integer in the set S of all linear combinations of a and b is exactly (a, b).

(*a*) $(6, 15) = 3$ (*b*) $(12, 17)=1$.

15. (a) This is a calculation.

(b) At the first step, for example, by Exercise 13 we have $(a, b) = (524, 148) = (148, 80) = (b, r)$. The same applies at each of the remaining steps. So at the final step, we have $(8, 4) = (4, 0)$; putting this string of equalities together gives

$$(524, 148) = (148, 80) = (80, 68) = (68, 12) = (12, 8) = (8, 4) = (4, 0).$$

But by Example 4, $(4, 0) = 4$, so that $(524, 148) = 4$.

(c) $1003 = 56 \cdot 17 + 51$, $56 = 51 \cdot 1 + 5$, $51 = 5 \cdot 10 + 1$, $5 = 1 \cdot 5 + 0$. Thus $(1003, 56) = (1, 0) = 1$.

(d) $322 = 148 \cdot 2 + 26$, $148 = 26 \cdot 5 + 18$, $26 = 18 \cdot 1 + 8$, $18 = 8 \cdot 2 + 2$, $8 = 2 \cdot 4 + 0$, so that $(322, 148) = (2, 0) = 2$.

(e) $5858 = 1436 \cdot 4 + 114$, $1436 = 114 \cdot 12 + 68$, $114 = 68 \cdot 1 + 46$, $68 = 46 \cdot 1 + 22$, $46 = 22 \cdot 2 + 2$, $22 = 2 \cdot 11 + 0$, so that $(5858, 1436) = (2, 0) = 2$.

(f) $68 = 148 - (524 - 148 \cdot 3) = -524 + 148 \cdot 4$.

(g) $12 = 80 - 68 \cdot 1 = (524 - 148 \cdot 3) - (-524 + 148 \cdot 4) \cdot 1 = 524 \cdot 2 - 148 \cdot 7$.

(h) $8 = 68 - 12 \cdot 5 = (-524 + 148 \cdot 4) - (524 \cdot 2 - 148 \cdot 7) \cdot 5 = -524 \cdot 11 + 148 \cdot 39$.

(i) $4 = 12 - 8 = (524 \cdot 2 - 148 \cdot 7) - (-524 \cdot 11 + 148 \cdot 39) = 524 \cdot 13 - 148 \cdot 46$.

(j) Working the computation backwards gives $1 = 1003 \cdot 11 - 56 \cdot 197$.

16. Let $a = da_1$ and $b = db_1$. Then a_1 and b_1 are integers and we are to prove: $(a_1, b_1) = 1$. By Theorem 1.3 there exist integers u, v such that $au + bv = d$. Substituting and cancelling we find that $a_1u + b_1v = 1$. Therefore any common divisor of a_1 and b_1 must also divide this linear combination, so it divides 1. Hence $(a_1, b_1) = 1$.

17. Since $b \mid c$, we know that $c = bt$ for some integer t. Thus $a \mid c$ means that $a \mid bt$. But then Theorem 1.4 tells us, since $(a, b) = 1$, that $a \mid t$. Multiplying both sides by b gives $ab \mid bt = c$.

18. Let $d = (a, b)$ so there exist integers x, y with $ax + by = d$. Note that $cd \mid (ca, cb)$ since cd divides ca and cb. Also $cd = cax + cby$ so that $(ca, cb) \mid cd$. Since these quantities are positive we get $cd = (ca, cd)$.

19. Let $d = (a, b)$. Since $b + c = aw$ for some integer w, we know c is a linear combination of a and b so that $d \mid c$. But then $d \mid (b, c) = 1$ forcing $d = 1$. Similarly $(a, c) = 1$.

20. Let $d = (a, b)$ and $e = (a, b + at)$. Since $b + at$ is a linear combination of a and b, $d \mid (b + at)$ so that $d \mid e$. Similarly since $b = a(-t) + (b + at)$ is a linear combination of a and $b + at$ we know $e \mid b$ so that $e \mid d$. Therefore $d = e$.

21. Answered in the text.

22. Let $d = (a, b, c)$. Claim: $(a, d) = 1$. [Proof: (a, d) divides d so it also divides c. Then $(a, d) \mid (a, c) = 1$ so that $(a, d)= 1$.] Similarly $(b, d)= 1$. But $d \mid ab$ and $(a, d) = 1$ so that Theorem 1.5 implies that $d \mid$ b. Therefore $d = (b. d) = 1$.

23. Define the powers b^n recursively as follows: $b^1 = b$ and for every $n \geq 1$, $b^{n+1} = b \cdot b^n$. By hypothesis $(a, b^1) = 1$. Given $k \geq 1$, assume that $(a, b^k) = 1$. Then $(a, b^{k+1}) = (a, b \cdot b^k) = 1$ by Exercise 24. This proves that $(a, b^n) = 1$ for every $n \geq 1$.

24. Let $d = (a, b)$. If $ax + by = c$ for some integers x, y then c is a linear combination of a and b so that $d \mid c$. Conversely suppose c is given with $d \mid$ c, say $c = dw$ for an integer w. By Theorem 1.3 there exist integers u, v with $d = au + bv$. Then $c = dw = auw + bvw$ and we use $x = uw$ and $y = vw$ to solve the equation.

25. (a) Given $au + bv = 1$ suppose $d = (a, b)$. Then $d \mid a$ and $d \mid b$ so that d divides the linear combination $au + bv = 1$. Therefore $d = 1$.
    (b) There are many examples. For instance if $a = b = d = u = v = 1$ then $(a, b) = (1, 1)= 1$ while $d = au + bv = 1 + 1 = 2$.

26. Let $d = (a, b)$ and express $a = da_1$ and $b = db_1$ for integers a_1, b_1. By Exercise 16, $(a_1, b_1) = 1$. Since $a \mid c$ we have $c = au = da_1u$ for some integer u. Similarly $c = bv = db_1v$ for some integer v. Then $a_1u = c/d = b_1V$ and Theorem 1.5 implies that $a_1 \mid v$ so that $v = a_1w$ for some integer w. Then $c = da_1b_1w$ so that $cd = d^2a_1b_1w = abw$ and $ab \mid cd$.

27. Answered in the text.

28. Suppose the integer consists of the digits $a_na_{n-1}\ldots a_1a_0$. Then the number is equal to

$$\sum_{k=0}^{n} a_k 10^k = \sum_{k=0}^{n} a_k(10^k - 1) + \sum_{k=0}^{n} a_k.$$

Now, the first term consists of terms with factors of the form $10^k - 1$, all of which are of the form $999\ldots99$, which are divisible by 3, so that the first term is always divisible by 3. Thus $\sum_{k=0}^{n} a_k 10^k$ is divisible by 3 if and only if the second term $\sum_{k=0}^{n} a_k$ is divisible by 3. But this is the sum of the digits.

29. This is almost identical to Exercise 28. Suppose the integer consists of the digits $a_na_{n-1}\ldots a_1a_0$. Then the number is equal to

$$\sum_{k=0}^{n} a_k 10^k = \sum_{k=0}^{n} a_k(10^k - 1) + \sum_{k=0}^{n} a_k.$$

Now, the first term consists of terms with factors of the form $10^k - 1$, all of which are of the form $999\ldots99$, which are divisible by 9, so that the first term is always divisible by 9. Thus $\sum_{k=0}^{n} a_k 10^k$ is divisible by 9 if and only if the second term $\sum_{k=0}^{n} a_k$ is divisible by 9. But this is the sum of the digits.

30. Let $S = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n : x_1\ x_2, ..., x$ are integers$\}$. As in the proof of Theorem 1.3, S does contain some positive elements (for if $a_i \neq 0$ then $a_i^2 \in S$ is positive). By the Well Ordering Axiom this set S contains a smallest positive element, which we call t. Suppose $t = a_1u_1 + a_2u_2 + \cdots + a_nu_n$ for some integers u_i.
Claim. $t = d$. The first step is to show that $t \mid a_1$. By the division algorithm there exist integers q and r such that $a_1 = tq + r$ with $0 \leq r < t$. Then $r = a_1 - tq = a_1(1 - u_1q) + a_2(-u_2q) + \cdots + a_n(-u_nq)$ is an element of S. Since $r < t$ (the smallest positive element of S), we know r is not positive. Since $r \geq 0$ the only possibility is $r = 0$. Therefore $a_1 = tq$ and $t \mid a_1$. Similarly we have $t \mid a_j$ for each j, and t is a common divisor of $a_1, a_2, \cdots, a_n$. Then $t \leq d$ by definition.

On the other hand d divides each a_i so d divides every integer linear combination of $a_1, a_2, \cdots, a_n$. In particular, $d \mid t$. Since $t > 0$ this implies that $d \leq t$ and therefore $d = t$.

31. (a) $[6, 10] = 30$; $[4, 5, 6, 10] = 60$; $[20, 42] = 420$, and $[2, 3, 14, 36, 42] = 252$.

(b) Suppose $a_i \mid t$ for $i = 1, 2, \ldots, k$, and let $m = [a_1, a_2, \ldots, a_k]$. Then we can write $t = mq + r$ with $0 \leq r < m$. For each i, $a_i \mid t$ by assumption, and $a_i \mid m$ since m is a common multiple of the a_i. Thus $a_i \mid (t - mq) = r$. Since $a_i \mid r$ for each i, we see that r is a common multiple of the a_i. But m is the smallest positive integer that is a common multiple of the a_i; since $0 \leq r < m$, the only possibility is that $r = 0$ so that $t = mq$. Thus any common multiple of the a_i is a multiple of the least common multiple.

32. First suppose that $t = [a, b]$. Then by definition of the least common multiple, t is a multiple of both a and b, so that $t \mid a$ and $t \mid b$. If $a \mid c$ and $b \mid c$, then c is also a common multiple of a and b, so by Exercise 31, it is a multiple of t so that $t \mid c$.

Conversely, suppose that t satisfies the conditions (i) and (ii). Then since $a \mid t$ and $b \mid t$, we see that t is a common multiple of a and b. Choose any other common multiple c, so that $a \mid c$ and $b \mid c$. Then by condition (ii), we have $t \mid c$, so that $t \leq c$. It follows that t is the least common multiple of a and b.

33. Let $d = (a, b)$, and write $a = da_1$ and $b = db_1$. Write $m = \frac{ab}{d} = \frac{da_1db_1}{d} = da_1b_1$. Since a and b are both positive, so is m, and since $m = da_1b_1 = (da_1)b_1 = ab_1$ and $m = da_1b_1 = (db_1)a_1 = ba_1$, we see that m is a common multiple of a and b. Suppose now that k is a positive integer with $a \mid k$ and $b \mid k$. Then $k = au = bv$, so that $k = da_1u = db_1v$. Thus $\frac{k}{d} = a_1u = b_1v$. By Exercise 16, $(a_1, b_1) = 1$, so that $a_1 \mid v$, say $v = a_1w$. Then $k = db_1v = db_1a_1w = mw$, so that $m \mid k$. Thus $m \leq k$. It follows that m is the least common multiple. But by construction, $m = \frac{ab}{(a,b)} = \frac{ab}{d}$.

34. (a) Let $d = (a, b)$. Since $d \mid a$ and $d \mid b$, it follows that $d \mid (a + b)$ and $d \mid (a - b)$, so that d is a common divisor of $a + b$ and $a - b$. Hence it is a divisor of the greatest common divisor, so that $d = (a, b) \mid (a + b, a - b)$.

(b) We already know that $(a, b) \mid (a+b, a-b)$. Now suppose that $d = (a+b, a-b)$. Then $a+b = dt$ and $a - b = du$, so that $2a = d(t + u)$. Since a is even and b is odd, d must be odd. Since $d \mid 2a$, it follows that $d \mid a$. Similarly, $2b = d(t - u)$, so by the same argument, $d \mid b$. Thus d is a common divisor of a and b, so that $d \mid (a, b)$. Thus $(a, b) = (a + b, a - b)$.

(c) Suppose that $d = (a + b, a - b)$. Then $a + b = dt$ and $a - b = du$, so that $2a = d(t + u)$. Since a and b are both odd, $a + b$ and $a - b$ are both even, so that d is even. Thus $a = \frac{d}{2}(t + u)$, so that $\frac{d}{2} \mid a$. Similarly, $\frac{d}{2} \mid b$, so that $\frac{d}{2} = \frac{(a+b,a-b)}{2} \mid (a, b) \mid (a + b, a - b)$. Thus $(a, b) = \frac{(a+b,a-b)}{2}$ or $(a, b) = (a + b, a - b)$. But since (a, b) is odd and $(a + b, a - b)$ is even, we must have $\frac{(a+b,a-b)}{2} = (a, b)$, or $2(a, b) = (a + b, a - b)$.