1 Elementary number theory

Divisibility

Exercise 1.1 (Division Algorithm)**.** You are asked to prove Theorem 1.4, the Division Algorithm:

For any positive integers $a \geqslant m$, there exist unique integers q and r such that

$$a = qm + r \qquad \text{and } 0 \leqslant r < m.$$

Prove this using the following steps:

(a) **(Existence)** Given $a \geqslant m \geqslant 1$, consider the set

$$S = \{a - km : \ k \in \mathbf{Z} \text{ and } a - km \geqslant 0\}.$$

Prove that S is a non-empty subset of $\mathbf{N}$ and deduce from the Well-Ordering Property of $\mathbf{N}$ that S has a minimal element r. Prove that $0 \leqslant r < m$.

Let q be the corresponding value of k.

(b) **(Uniqueness)** Prove that q and r are unique, in other words if q, q', r, r' satisfy

$$a = qm + r = q'm + r' \qquad \text{and } 0 \leqslant r < m, 0 \leqslant r' < m,$$

then $q = q'$ and $r = r'$.

Exercise 1.2. We explore some of the basic properties of divisibility.

(a) Prove that if $a, b, c \in \mathbf{Z}$ such that $a \mid b$ and $b \mid c$, then $a \mid c$.

(b) Prove that if $d \mid a$ and $d \mid b$, then for any $u, v \in \mathbf{Z}$ we have $d \mid (ua + vb)$.

(c) Let $g = \gcd(a, b)$ and suppose $d \in \mathbf{Z}$ is such that $d \mid a$ and $d \mid b$. Prove that $g \mid d$.

Exercise 1.3. Prove that if $d \mid n$ and $n \mid d$, then $d = n$. Here we're assuming d and n are positive. What happens if they're allowed to be negative?

Exercise 1.4. For any $m, n \in \mathbf{Z}_{\geqslant 1}$, prove that

$$\gcd(m, n) = 1 \quad \iff \quad \gcd(m^2, n^2) = 1.$$

Exercise 1.5. Suppose $a, b \in \mathbf{Q}_{>0}$ are such that $a^2 + b^2 = 1$. Prove that if $a = \dfrac{a_1}{a_2}$ and $b = \dfrac{b_1}{b_2}$ with $a_1, a_2, b_1, b_2 \in \mathbf{Z}_{\geqslant 1}$ are expressed in lowest terms, then $a_2 = b_2$.

Exercise 1.6. Let $m \in \mathbf{Z}_{\geqslant 1}$. Prove that if integers a, b, c, d satisfy $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \qquad \text{and} \qquad ac \equiv bd \pmod{m}.$$

Exercise 1.7. Do the following Diophantine equations have a solution?

(a) $24x - 18y = 8$

(b) $5x + 2y = 0$

(c) $5x + 2y = 1$

(d) $5x + 2y = 6$

(e) $5x - 2y = 6$.

Exercise 1.8. Express the number 5 as a $\mathbf{Z}$-linear combination of 17 and 47. In other words, find integers x and y such that $17x + 47y = 5$.

Exercise 1.9. Show that there is no non-constant polynomial with integer coefficients that "outputs" only prime numbers. More precisely, prove that if f is a non-constant polynomial with integer coefficients, then there exists $n \in \mathbf{Z}$ such that $f(n)$ is not prime.

[**Hint**: By contradiction: given such f, let $p = f(0)$. What can you say about $f(p)$, $f(2p)$, $f(3p)$,...?]

Exercise 1.10. True or false?

(a) If n is composite, then $2^n - 1$ is composite.

(b) If n is prime, then $2^n - 1$ is prime.

Exercise 1.11. Prove that congruence modulo n is an *equivalence relation*. In other words, prove the following:

(a) $a \equiv a \mod m$;

(b) if $a \equiv b \mod m$, then $b \equiv a \mod m$;

(c) if $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \bmod m$.

Exercise 1.12. Prove that the Diophantine equation $x^2 - xy - 2y^2 = -1$ has no integer solutions.

[**Hint**: Consider a congruence modulo a cleverly chosen integer m. You may have to consider a few small m before finding an appropriate one.]

Abelian groups

Exercise 1.13. Let G be an abelian group. (Look up the precise definition in the notes.)

(a) Prove that the neutral element 0 is unique.

(b) Let $g \in G$. Prove that the inverse of g is unique.

[**Hint**: The process for showing that something is unique is: assume there are two things x and x' with the given properties, then prove that $x = x'$.]

Exercise 1.14. Let G be an abelian group and H a subgroup.
Given $g \in G$, we define a **subset** of G by

$$g + H = \{g + h : \ h \in\}.$$

(a) Prove that for any $g_1, g_2 \in G$ there is a bijective function $g_1 + H \longrightarrow g_2 + H$, hence that $\#(g_1 + H) = \#(g_2 + H)$.

(b) Prove that for any $g_1, g_2 \in G$ we have that

$$\text{either} \quad (g_1 + H) \cap (g_2 + H) = \varnothing \quad \text{or} \quad g_1 + H = g_2 + H.$$

(c) Conclude that $\#H$ divides $\#G$.

Exercise 1.15. Let $f : \ G \longrightarrow H$ be a group homomorphism between abelian groups.

(a) Prove that $f(0_G) = 0_H$.

(b) Prove that for every $g \in G$ we have $f(-g) = -f(g)$.

Exercise 1.16. Let $f : \ G \longrightarrow H$ be a group homomorphism between abelian groups.

(a) Prove that the kernel $\ker f$ is a subgroup of G.

(b) Prove that the image $\mathsf{im}\, f$ is a subgroup of H.

Exercise 1.17. Find the kernel and the image of

(a) the exponential map $f : \ \mathbf{R} \longrightarrow \mathbf{S}^1$ defined in Example 1.25;

(b) the reduction modulo m map $f : \ \mathbf{Z} \longrightarrow \mathbf{Z}/m\mathbf{Z}$ defined in Example 1.26.

Exercise 1.18. Let G be an abelian group and take $g \in G$.

(a) Prove that if the order of g is $m \in \mathbf{Z}_{\geqslant 1}$, then $\langle g \rangle$ is isomorphic to $\mathbf{Z}/m\mathbf{Z}$.

(b) Prove that if the order of g is infinite, then $\langle g \rangle$ is isomorphic to $\mathbf{Z}$.

Exercise 1.19. Prove that the abelian groups $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$ and $(\mathbf{Z}/8\mathbf{Z})^\times$ are isomorphic.

Answers

Solution 1.1. (a) S is non-empty because $a - 0 \cdot m = a \in S$. By the Well-Ordering Property of $\mathbf{N}$, S has a minimal element r. Then $r = a - qm \geqslant 0$ for some $q \in \mathbf{Z}$. Seeking a contradiction, suppose that $r \geqslant m$. Then $r - m \geqslant 0$ and

$$r - m = a - (q+1)m \in S.$$

We have found $r - m$ is in S, contradicting the minimailty of r. Hence $0 \leqslant r \leqslant m$.

(b) Without loss of generality, $q \geqslant q'$. Observe that

$$qm + r = q'm + r' \implies r' - r = (q - q')m.$$

By assumption $r' - r < m$ and therefore $(q-q')m < m$ which implies $q - q' < 1$, Since $q - q'$ is a non-negative integer less than 1 we must have $q = q'$ and therefore $r = r'$.

Solution 1.2. (a) There exists $m, n \in \mathbf{Z}$ such that $b = ma$ and $c = nb$. Substituting the first into the second we get $c = n(ma) = (nm)a$ and thus $a \mid c$.

(b) There exists $m, n \in \mathbf{Z}$ such that $a = md$ and $b = nd$. Then

$$ua + vb = u(md) + v(nd) = (am + vn)d,$$

hence $d \mid ua + vb$.

(c) The Euclidean algorithm provides $x, y \in \mathbf{Z}$ such that $xa + yb = g$. Applying the previous part, we get

$$d \mid xa + yb = g.$$

Solution 1.3. If $d \mid n$ then there exists a positive integer k such that

$$d = kn. \tag{1}$$

If $n \mid d$ then there exists a positive integer j such that

$$n = jd. \tag{2}$$

Substituting (1) into (2) results in

$$n = jkn$$

and hence

$$jk = 1. \tag{3}$$

Since j, k are positive integers, we must have $j = k = 1$ and hence from (1)

$$d = n.$$

If n, d are allowed to be negative then j, k may be negative. This means solutions to (3) are given by

$$j = k = 1 \quad \text{or} \quad j = k = -1$$

so that $d = \pm n$.

Solution 1.4. ($\Rightarrow$): Suppose $\gcd(m,n)=1$ but $\gcd(m^2,n^2)>1$, then there exists a prime number p that divides $\gcd(m^2,n^2)$. So $p \mid m^2$; since p is prime this implies that $p \mid m$. Similarly we see that $p \mid n$. Hence p is a common divisor of m and n, hence it divides $\gcd(m,n)=1$, contradiction.

($\Leftarrow$): Suppose $\gcd(m^2,n^2)=1$ but $\gcd(m,n)>1$, then there exists a prime number p that divides $\gcd(m,n)$. Then $p \mid m$, so certainly $p \mid m^2$. Also $p \mid n$, so $p \mid n^2$. Therefore p is a common divisor of m^2 and n^2, hence it divides $\gcd(m^2,n^2)=1$, contradiction.

Solution 1.5. Substituting into $a^2+b^2=1$ and clearing denominators, we get

$$a_1^2 b_2^2 + b_1^2 a_2^2 = a_2^2 b_2^2.$$

In particular,

$$a_1^2 b_2^2 = a_2^2(b_2^2 - b_1^2).$$

Since $\gcd(a_1,a_2)=1$ we have that $\gcd(a_1^2,a_2^2)=1$, so the above equation tells us that $a_2^2 \mid b_2^2$.

On the other hand, we can rewrite the first equation as

$$b_1^2 a_2^2 = b_2^2(a_2^2 - a_1^2).$$

Since $\gcd(b_1,b_2)=1$ we have that $\gcd(b_1^2,b_2^2)=1$, tho the above equation tells us that $b_2^2 \mid a_2^2$.

Hence $a_2^2 = b_2^2$, so that $a_2 = b_2$ by positivity.

Solution 1.6. We have integers k, ℓ such that $a-b=km$ and $c-d=\ell m$. The addition statement follows from:

$$(a-b)+(c-d) = (a+c)-(b+d) = (k+\ell)m.$$

The multiplicative statement follows from:

$$\begin{aligned} ac - bd &= (km+b)(\ell m + d) - bd \\ &= (mk\ell + kd + \ell b)m. \end{aligned}$$

Solution 1.7.

(a) No, since $\gcd(24,18)=6$ and 6 does not divide 8.

(b) Yes, $(x,y)=(-2,5)$

(c) Yes, $(x,y)=(1,-2)$

(d) Yes, $(x,y)=(6,-12)$

(e) Yes, $(x,y)=(6,12)$.

Solution 1.8. By the extended Euclidean algorithm $(x,y)=(-11,4)$ is a solution to $17x+47y=1$. Hence $(x,y)=(-55,20)$ is a solution to $17x+47y=5$.

Solution 1.9. Write

$$f(x) = c_n x^n + \cdots + c_1 x + c_0.$$

If $p = f(0)$, then $c_0 = p$. Then for any $a \in \mathbf{Z}$ we have

$$f(ap) = c_n (ap)^n + \cdots + c_a (ap) + p,$$

clearly a multiple of p. By assumption then, we must have $f(ap) = p$ for all $a \in \mathbf{Z}$. But then the polynomial equation $f(x) - p = 0$ has infinitely many distinct solutions $\{ap : \ a \in \mathbf{Z}\}$, which forces $f(x) - p = 0$ for all x, hence $f(x) = p$, contradicting the fact that f should be non-constant.

Solution 1.10.

(a) This is true.

If $n = 2m$ is even and composite, so $m > 1$, we have

$$2^n - 1 = (2^m)^2 - 1 = (2^m - 1)(2^m + 1),$$

and both factors are > 1.

If $n = ab$ is odd, with $a, b > 1$, we have

$$2^n - 1 = (2^a)^b - 1 = (2^a - 1)\left((2^a)^{b-1} + \cdots + 2^a + 1\right),$$

and again both factors are > 1.

(b) This is false, for instance

$$2^{11-1} = 23 \cdot 89.$$

Solution 1.11.

Solution 1.12. Reducing mod 3 gives $x^2 + 2xy + y^2 \equiv 2 \mod 3$ which implies

$$(x + y)^2 \equiv 2 \mod 3,$$

but 2 is not a square modulo 3.

Solution 1.13. (a) Suppose there exists two neutral elements 0 and $0'$. Then using the property of neutral elements we get:

$$0 = 0 + 0' = 0'.$$

(b) Suppose h and k are both inverses of g. Then using the property of inverses and associativity of the group operation:

$$h = h + 0 = h + (g + k) = (h + g) + k = 0 + k = k.$$

Solution 1.14.

(a)

(b)

(c)

Solution 1.15. (a) We have $f(0_G) = f(0_G + 0_G) = f(0_G) + f(0_G)$, and so adding the inverse of $f(0_G)$ to both sides we get $f(0_G) = 0_H$.

(b) Using the previous part, we have

$$0_H = f(0_G) = f(g + (-g)) = f(g) + f(-g),$$

which shows that $f(-g)$ is the inverse of $f(g)$.

Solution 1.16. (a) By Exercise 1.15, we know $0_G \in \ker f$. Now suppose that $g_1, g_2 \in \ker f$. Then using Exercise 1.15 again:

$$f(g_1 - g_2) = f(g_1) - f(g_2) = 0 - 0 = 0,$$

and so $g_1 - g_2 \in \ker f$, hence $\ker f$ is a subgroup of G.

(b) Using Exercise 1.15 again, we have $f(0_G) = 0_H$, so $0_H \in \operatorname{im} f$. Now suppose $h_1, h_2 \in \operatorname{im} f$. Then there exists $g_1, g_2 \in G$ such that $f(g_1) = h_1$ and $f(g_2) = h_2$. Then

$$h_2 - h_1 = f(g_2) - f(g_1) = f(g_2 - g_1),$$

so $h_2 - h_1 \in \operatorname{im} f$. Thus $\operatorname{im} f$ is a subgroup of H.

Solution 1.17. (a) First we compute the kernel. If $\theta \in \ker f$, then $e^{i\theta} = 1$ and so $\theta \in \{2\pi k : k \in \mathbf{Z}\} = 2\pi\mathbf{Z}$, and clearly all $\theta \in 2\pi\mathbf{Z}$ are in the kernel, thus $\ker f = 2\pi\mathbf{Z}$.

We claim the image of f is the set $\mathbf{S}^1$. Given $z \in \mathbf{S}^1$, then $f(\operatorname{Arg} z) = z$, showing $z \in \operatorname{im} f$.

(b) If $a \in \ker f$, then the remainder of the division of a by m is zero, which means $m \mid a$. Hence $a \in \{mk : k \in \mathbf{Z}\} = m\mathbf{Z}$. Clearly all $a \in m\mathbf{Z}$ are in the kernel and so $\ker f = m\mathbf{Z}$.

Given $r \in \mathbf{Z}/m\mathbf{Z}$, then $0 \leqslant r < m$ and so the remainder of the division of r by m is just r and so $f(r) = r$, hence $\operatorname{im} f = \mathbf{Z}/m\mathbf{Z}$.

Solution 1.18.

(a)

(b)

Solution 1.19. The map $f : (\mathbf{Z}/8\mathbf{Z})^\times \longrightarrow (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$ given by

$$\begin{aligned} 1 &\mapsto (0,0) \\ 3 &\mapsto (1,0) \\ 5 &\mapsto (0,1) \\ 7 &\mapsto (1,1), \end{aligned}$$

is a bijective homomorphism.