Solutions to Nathanson's Elementary Methods in Number Theory

H. Ronald

Contents

1 Divisibility and Primes

1.1 Division Algorithm

Exercises 1-5 are straightforward. Exercise 6-7 is easily solved using a method generalized from the method of converting decimal numbers to binary numbers. Exercise 8 is again straightforward if we put $n = 2k$.

EXERCISE 9. *Prove that n is odd, then $n^2 - 1$ is divisible by 8.*

SOLUTION. We put $n = 2k - 1$ for some $k \in \mathbb{Z}$. Then $n^2 - 1$ equals $4k^2 - 4k$, that is, $4k(k-1)$. Since either k or $k - 1$ is even, the product $k(k-1)$ is even. It follows that $n^2 - 1$ is divisible by 8. ■

EXERCISE 10. *Prove that $n^3 - n$ is divisible by 6 for every integer n.*

SOLUTION. By expanding $n^3 - n$ to $n(n-1)(n+1)$, we see that it is a sum of 3 consecutive integers. Clearly, at least one of them is a even number (say $2k$) and another one is a multiple of 3 (say $3h$). Therefore, $n^3 - n$ has $6hk$ as its factor and hence is divisible by 6. ■

Exercise 11 is straightforward if we put $a = dk$. Exercises 12-14 are easily solved using a similar approach.

EXERCISE 15. *Prove by induction that $n \leq 2^{n-1}$ for all positive integers n.*

SOLUTION. The case of $n = 1$ is easily verified. Suppose the proposition holds for $n = k$ for some $k \in \mathbb{Z}, k > 0$. Then $k \leq 2^{k-1}$, which implies, $k + 1 \leq 2^{k-1} + 1 \leq 2^{k+1-1}$ (because adding 1 to a positive integer cannot make it greater than multiplying the same integer by 2). Therefore, by induction, the proposition is true for all positive integers n. ■

Exercises 16-17 are easy exercises of using induction.

EXERCISE 19. *Let a and d be integers with $d \geq 1$. Prove that there exist unique integers q' and r' such that $a = dq' + r'$ and $-d/2 < r' \leq d/2$.*

SOLUTION. Let

Exercise 20 is a straightforward computation using the definition of binomial coefficient.

EXERCISE 21. *Prove that the product of any k consecutive integers is always divisible by $k!$.*

SOLUTION.

EXERCISE 22. *Let $m_0, m_1, m_2, \ldots$ be a strictly increasing sequence of positive integers such that $m_0 = 1$ and m_i divides m_{i+1} for all $i \geq 0$. Prove that every positive integer n can be represented uniquely in the form $n = \sum_{i=0}^{\infty} a_i m_i$, where $0 \leq a_i \leq m_{i+1}/m_i - 1$ for all $i \geq 0$ and $m_i = 0$ for all but finitely many integers i.*

SOLUTION.

Exercise 23-24 follows trivially from Exercise 22. Exercise 25-26 are simple applications of well-ordering of natural numbers.

1.2 Greatest Common Divisors

Exercises 1-3 are straightforward using Euclid's division algorithm.

EXERCISE 4. *Construct four relatively prime integers a, b, c, d such that no three of them are relatively prime.*

SOLUTION. Consider the canonical decompositions (prime factorizations): $2 \cdot 3 \cdot 5$, $3 \cdot 5 \cdot 7$, $5 \cdot 7 \cdot 11$ and $7 \cdot 11 \cdot 13$. It is easy to verify that all four of them are relatively prime but no three of them are relatively prime. ∎

The approach outlined above may be generalized to any number of integers. Exercise 5 becomes trivial once we realize that n and $n + 2$ cannot have a common factor greater than 2. Exercises 6-8 are all similar (the idea is to use Bézout's identity), so we will solve only Exercise 8.

EXERCISE 8. *Prove that $n! + 1$ and $(n + 1)! + 1$ are relatively prime for every integer n.*

SOLUTION. Let $a = n! + 1$ and $b = (n+1)! + 1$. Let $x = n + 1$ and $y = -n$. Then $xa + yb = 1$, that is $\gcd(a, b) = 1$. The proposition follows. ∎

EXERCISE 9. *Let a, b and d be positive integers. Prove that if $(a, b) = 1$ and d divides a, then $(d, b) = 1$.*

SOLUTION. Suppose, for the sake of contradiction, $\gcd(d, b) = g$ for some $g \neq 1$. Then $b = gh$ and $d = gk$ for some $h, k \in \mathbb{Z}$. Since d divides a, we may write $a = dq = gkq$ for some $q \in \mathbb{Z}$. It follows that $\gcd(a, b) = \gcd(gkq, gh) \neq 1$ since $g \neq 1$ is a common factor, which contradicts our premise. The proposition follows. ∎

Exercises 10-12 are simple applications of divisibility and gcd. Exercise 13 is easily solved using induction on the size n of the set A (consider the base cases of $n = 1$ and $n = 2$).

EXERCISE 14. *Let a, b, c, d be integers such that $ad - bc = 1$. For integers u and v, define $u' = au + bv$ and $v' = cu + dv$. Prove that $(u, v) = (u', v')$.*

SOLUTION.

Exercise 15 is straightforward in that reflexivity follows from choosing $t = 1$, symmetry follows from considering $1/t$ and transitivity follows from repeated multiplication.

EXERCISE 16. *Consider $(25/6, -5, 10/3) \in \mathbb{Q}^3$. Find all triples (a_0, a_1, a_2) of relatively prime integers such that $(a_0, a_1, a_2) \sim (25/6, -5, 10/3)$.*

SOLUTION. Multiplication by $t = 6$ convinces us to look for triplets (a_0, a_1, a_2) of relatively prime integers such that $(a_0, a_1, a_2) \sim (25, -5, 10) \sim (5, -1, 2)$. We need to consider only the integral values of t. Clearly, $(5, -1, 2)$ is one such triplet. The other triplet is $(-5, 1, -2)$. There are no other triplets since any value of $t \neq \pm 1$ ensures that a_0, a_1, a_2 are no longer relatively prime since, of course, t will be a common factor. ∎

Exercise 17 is similar to how we treated Exercise 16 (above). Exercises 18-19 are straightforward — we just verify the axioms of a group (closure, existence of identity and inverse).

4

EXERCISE 20. *Let H be a nonempty subset of an additive abelian group G. Prove that H is a subgroup if and only if $x - y \in H$ for all $x, y \in H$.*

SOLUTION.

Exercise 21 follows trivially from closure under multiplication (and addition). Exercises 22-23 are simple applications of elementary set theory and group axioms.

EXERCISE 24. *Prove that every nonzero subgroup of $\mathbb{Z}$ is isomorphic to $\mathbb{Z}$.*

SOLUTION. Every subgroup of $\mathbb{Z}$ is of the form $d\mathbb{Z}$ for some $d \in \mathbb{Z}, d \geq 0$. Consider the map $\varphi : d\mathbb{Z} \to \mathbb{Z}$ defined by $\varphi(d \cdot z) = z$ or equivalently, $\varphi(z) = z/d$. It is easily checked that φ satisfies the conditions of a homomorphism and that φ is a bijection, that is, φ gives the isomorphism. ∎

EXERCISE 25. *Let G be the set of all matrices of the form*

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},$$

with $a \in \mathbb{Z}$ and matrix multiplication as the binary operation. Prove that G is an abelian group isomorphic to $\mathbb{Z}$.

SOLUTION. Let $a, b \in \mathbb{Z}$. Then

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}.$$

Closure under multiplication and commutativity follows trivially. The identity element is then the identity matrix of order 2 itself. The inverse element of $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ is $\begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}$. Thus G is an abelian group under matrix multiplication.

From the above discussion, it is clear that no information is lost or gained when we re-write the matrix $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ as simply a and replace matrix multiplication by the usual addition in $\mathbb{Z}$ — we are simply re-writing the elements and group operation using a different notation. Therefore, $(G, \times)$ is isomorphic to $(\mathbb{Z}, +)$. The isomorphism is formally established by considering the natural map $\varphi : G \to \mathbb{Z}$ defined by

$$\varphi : \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \rightsquigarrow a.$$

That φ is a homomorphism is easily checked. The bijectivity of φ follows from considering the inverse map φ^{-1}. ∎

Exercise 26 is straightforward by considering a particular case (example).

EXERCISE 27. *Let $\mathbb{R}$ be the additive group of real numbers and $\mathbb{R}^+$ the multiplicative group of positive real numbers. Let $\exp : \mathbb{R} \to \mathbb{R}^+$ be the exponential map $\exp(x) = e^x$. Prove that the exponential map is a group isomorphism.*

SOLUTION. The exponential map is a group homomorphism since $e^{x+y} = e^x \cdot e^y$ for all $x, y \in \mathbb{R}$. To see that it is also a bijection, we consider its inverse map, the natural logarithm, $\ln(z)$ for $z \in \mathbb{R}^+$. Therefore, the exponential map is a group isomorphism. ∎

EXERCISE 28. *Let G and H be groups which e the identity in H. Let $f : G \to H$ be a group homomorphism. The kernel of f is the set $f^{-1}(e) = \{x \in G : f(x) = e \in H\} \subset G$. The image of f is the set $f(G) = \{f(x) : x \in G\} \subset H$. Prove that the kernel of f is a subgroup of G, and the image of f is a subgroup of H.*

SOLUTION.

EXERCISE 29. *Define the map $f : \mathbb{Z} \to \mathbb{Z}$ by $f(n) = 3n$. Prove that f is a group homomorphism and determine the kernel and image of f.*

SOLUTION. Let $n, m \in \mathbb{Z}$. Then $f(n + m) = 3(n + m) = 3n + 3m = f(n) + f(m)$. Thus f is a group homomorphism. Let $k \in \ker(f)$. Then $f(k) = 0$, that is, $3k = 0$ which is true only when $k = 0$. Thus $\ker(f) = \{0\}$. Clearly the image of f is the set of multiples of 3. ∎

EXERCISE 30. *Let Γ_m denote the multiplicative group of mth roots of unity. Prove that the map $f : \mathbb{Z} \to \Gamma_m$ defined by $f(k) = e^{2\pi i k/m}$ is a group homomorphism. What is the kernel of this homomorphism?*

SOLUTION. Let $h, k \in \mathbb{Z}$. Then $f(h + k) = e^{2\pi i (h+k)/m} = e^{2\pi i h/m} \cdot e^{2\pi i k/m} = f(h) \cdot f(k)$. This proves the homomorphism. Let $k \in \ker(f)$. Then $f(k) = e^{2\pi i k/m} = 1$, which is true only when k/m is an integer. Thus $\ker(k)$ is the set of multiples of m. ∎

EXERCISE 31. *Let $G = [0, 1)$ be the interval of real numbers x such that $0 \le x < 1$. We define a binary operation $x * y$ for numbers $x, y \in G$ as follows:*

$$x * y = \begin{cases} x + y & \text{if } x + y < 1, \\ x + y - 1 & \text{if } x + y \ge 1. \end{cases}$$

Prove that G is an abelian group with this operation. This group is denoted by $\mathbb{R}/\mathbb{Z}$.

Define the map $f : \mathbb{R} \to \mathbb{R}/\mathbb{Z}$ by $f(t) = \{t\}$, where $\{t\}$ denotes the fractional part of t. Prove that f is a group homomorphism. What is the kernel of this homomorphism.

SOLUTION. Closure under $*$ follows from its definition. Clearly, the identity element is 0. It is easily checked that the inverse of a ($a \in G$) is $1 - a$. Commutativity follows from the definition of $*$ (since the expression remains the same when x and y are interchanged).

Let $s, t \in \mathbb{R}$. Then $f(s+t) = \{s+t\} = \{s\} * \{t\} = f(s) * f(t)$. This proves the homomorphism. Clearly $\ker(f)$ is the set $\mathbb{Z}$ of integers. ∎

1.3 The Euclidean Algorithm and Continued Fractions

Exercises 1-3 are simple computations using the Euclidean algorithm. Exercise 4 is a simple computational task. Exercises 5-6 become trivial once we expand the continued fractions.

EXERCISE 7. *Let $x = \langle a_0, a_1, \ldots, a_N \rangle$ be a finite simple continued fraction whose partial*

quotients a_i are integers, with $N \geq 1$ and $a_N \geq 2$. Let $[x]$ denote the integer part of x and $\{x\}$ the fractional part of x. Prove that $[x] = a_0$ and $\{x\} = 1/\langle a_1, a_2, \ldots, a_N \rangle$.

SOLUTION. Let p/q be the rational number corresponding to the finite simple continued fraction $x = \langle a_0, a_1, \ldots, a_N \rangle$. Since $a_0, a_1, \ldots, a_N$ are the partial quotients in the Euclidean algorithm on the division of p by q, it follows that $[x] = a_0$ (because a_0 is the quotient of p when divided by q). Also, $\{x\} = x - [x] = x = \langle a_0, a_1, \ldots, a_N \rangle - a_0 = 1/\langle a_1, a_2, \ldots, a_N \rangle$. ∎

EXERCISE 8.

Exercise 9 is obvious once we expand the continued fraction.

EXERCISE 10. *Let $\langle a_0, a_1, \ldots, a_N \rangle$ be a finite simple continued fraction. Define $p_0 = a_0$, $p_1 = a_1 a_0 + 1$, and $p_n = a_n p_{n-1} + p_{n-2}$ for $n = 2, \ldots, N$. Define $q_0 = 1$, $q_1 = a_1$, and $q_n = a_n q_{n-1} + q_{n-2}$ for $n = 2, \ldots, N$. Prove that*

$$\langle a_0, a_2, \ldots, a_n \rangle = \frac{p_n}{q_n}$$

for $n = 0, 1, \ldots, N$. The continued fraction $\langle a_0, a_1, \ldots, a_n \rangle$ is called the nth convergent of the continued fraction $\langle a_0, a_1, \ldots, a_N \rangle$.

SOLUTION. We prove this using induction on n. When $n = 1$, $p_1/q_1 = (a_1 a_0 + 1)/a_1$, which is the continued fraction $\langle a_0, a_1 \rangle$. Suppose the proposition holds for $n = k$.

Exercise 11 is a simple computation problem. The nth convergent should converge to the continued fraction as n grows larger.

EXERCISE 12. *Let $\langle a_0, a_1, \ldots, a_N \rangle$ be a finite simple continued fraction, and let p_n and q_n be the numbers defined in Exercise 10. Prove that*

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$$

for $n = 1, \ldots, N$. Prove that if $a_i \in \mathbb{Z}$ for $i = 0, 1, \ldots, N$, then $(p_n, q_n) = 1$ for $n = 0, 1, \ldots, N$.

SOLUTION.

EXERCISE 13. *Let $\langle a_0, a_1, \ldots, a_N \rangle$ be a finite simple continued fraction, and let p_n and q_n be the numbers defined in Exercise 10. Prove that*

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$$

for $n = 2, \ldots, N$.

SOLUTION.

EXERCISE. *Let $\langle a_0, a_1, \ldots, a_N \rangle$ be a finite simple continued fraction, and let p_n and q_n be the numbers defined in Exercise 10. Prove that the even convergents are strictly increasing, the odd convergents are strictly decreasing, and every even convergent is less than every odd convergent, that is,*

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots \leq x \leq \cdots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

SOLUTION.

EXERCISE 15. *We define a sequence of integers as follows:*

$$f_0 = 0,$$
$$f_1 = 1,$$
$$f_n = f_{n-1} + f_{n-2} \text{ for } n \geq 2.$$

The integer f_n is called the nth Fibonacci number. Compute the Fibonacci numbers f_n for $n = 2, 3, \ldots, 12$. Prove that $(f_n, f_{n+1}) = 1$ for all nonnegative integers n.

SOLUTION. The recurrence relation yields $f_2 = 1$, $f_3 = 2$, $f_4 = 3$, $f_5 = 5$, $f_6 = 8$, $f_7 = 13$, $f_8 = 21$, $f_9 = 34$, $f_{10} = 55$, $f_{11} = 89$, and $f_{12} = 144$. We now prove the proposition by induction. The base case for $n = 0$ holds trivially. Suppose the proposition holds for $n = k$ for some $k \in \mathbb{Z}, k > 0$. Then $\gcd(f_k, f_{k+1}) = 1$. But $f_{k+2} = f_{k+1} + f_k$. That is, any common divisor of f_{k+1} and f_k is also a common divisor of f_{k+2} and f_{k+1}. Therefore, $\gcd(f_{k+1}, f_{k+2}) = \gcd(f_k, f_{k+1}) = 1$. The proposition follows. ∎

In Exercises $16 - 23$, f_n denotes the nth Fibonacci number.

Exercise 16 is a simple computation problem.

EXERCISE 17. *Prove that*

$$f_1 + f_2 + \cdots + f_n = f_{n+2} - 1$$

for all positive integers n.

SOLUTION. We prove the proposition by induction. The base case for $n = 1$ holds trivially. Suppose the proposition holds for $n = k$ for some $k \in \mathbb{Z}, k > 1$. Then $f_1 + f_2 + \cdots + f_k = f_{k+2} - 1$. Adding f_{k+1} to both sides and using the Fibonacci recurrence relation yields $f_1 + f_2 + \cdots + f_{k+1} = f_{k+1+2} - 1$. The proposition follows. ∎

EXERCISE 18. *Prove that*

$$f_{n+1}f_{n-1} - f_n^2 = (-1)^n$$

for all positive integers n.

SOLUTION.

EXERCISE 19. *Prove that*

$$f_n = f_{k+1}f_{n-k} + f_k f_{n-k-1}$$

for all $k = 0, 1, \ldots, n$. Equivalently, $f_n = f_{n-1} + f_{n-2} = 2f_{n-2} + f_{n-3} = 3f_{n-3} + 2f_{n-4} = 5f_{n-4} + 3f_{n-5} \cdots$.

SOLUTION. The second part of the exercise follows readily from the Fibonacci recurrence relation. The coefficients follow the pattern $1, 1, 2, 3, 5, \ldots$. At every step we observe that the new coefficient is the sum of the previous two coefficients. These coefficients are the Fibonacci numbers f_n. Consequently, $f_n = f_{k+1}f_{n-k} + f_k f_{n-k-1}$. ∎

EXERCISE 20. *Prove that f_n divides f_{ln} for all positive integers l.*

SOLUTION. By the result of Exercise 19, we can write $f_{ln} = f$.

EXERCISE 21. *Prove that, for $n \geq 1$,*

$$\begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n.$$

SOLUTION. We prove the proposition by induction. The base case of $n = 1$ holds trivially. Suppose the proposition holds for $n = k$ for some $k \in \mathbb{Z}, k > 1$. Then

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{k+1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_{k+2} & f_{k+1} \\ f_{k+1} & f_k \end{pmatrix}.$$

The proposition follows. ∎

1.4 The Fundamental Theorem of Arithmetic

Exercises 1-4 are simple computation problems.

EXERCISE 5. *Compute the standard factorization of $15!$.*

SOLUTION. The primes not exceeding 15 are $2, 3, 5, 7, 11$ and 13. Then

$$v_2(15!) = \left[\frac{15}{2}\right] + \left[\frac{15}{4}\right] + \left[\frac{15}{8}\right] = 7 + 3 + 1 = 11,$$

$$v_3(15!) = \left[\frac{15}{3}\right] + \left[\frac{15}{9}\right] = 5 + 1 = 6,$$

$$v_5(15!) = \left[\frac{15}{5}\right] = 3,$$

$$v_7(15!) = \left[\frac{15}{7}\right] = 1,$$

$$v_{11}(15!) = \left[\frac{15}{11}\right] = 1,$$

$$v_{13}(15!) = \left[\frac{15}{13}\right] = 1.$$

Therefore, $15! = 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 13$. ∎

EXERCISE 6. *Prove that n, $n + 2$, $n + 4$ are all primes if and only if $n = 3$.*

SOLUTION. One direction is trivial: if $n = 3$, then 3, 5, and 7 are all primes. For the other direction, suppose n, $n + 2$, and $n + 4$ are all primes. Clearly n is odd. Also n is divisible by 3 (otherwise, either $n + 1$ (and consequently $n + 4$) or $n + 2$ will be divisible by 3 which cannot be true unless of course $n + 2$ is 3 itself in which case $n = 1$ which is impossible). Therefore $n = 3$ (because any other multiple of 3 is not prime). ∎

EXERCISE 7. *Prove that n, $n + 4$, $n + 8$ are all primes if and only if $n = 3$.*

SOLUTION. As in Exercise 6, one direction is trivial. Suppose n, $n + 4$, $n + 8$ are all primes. Suppose n is not divisible by 3. Then either $n+1$ or $n+2$ is divisible by 3. If $n+1$ is divisible by 3, then $3 \neq n + 4$ is also divisible by 3 which is absurd. If $n + 2$ is divisible by 3, then $3 \neq n + 8$ is divisible by 3 which is again absurd. Therefore $n = 3$. ∎

EXERCISE 8. *Let $n \geq 2$. Prove that $(n+1)! + k$ is composite for $k = 2, \ldots, n+1$. This shows that there exists arbitrarily long intervals of composite numbers.*

SOLUTION. The proposition follows since $(n + 1)! + k$ can also be written as $k[(k - 1)!(k + 1)(k + 2) \cdots (n + 1) + 1]$ which is divisible by k. ∎

EXERCISE 9. *Prove that $n^5 - n$ is divisible by 30 for every integer n.*

SOLUTION. Since $30 = 2 \cdot 3 \cdot 5$ we are done if we prove that $n^5 - n$, i.e., $n(n+1)(n-1)(n^2+1)$ has $2, 3$, and 5 as its prime factors. The cases for 2 and 3 are obvious since $n - 1$, n, $n + 1$ are three consecutive numbers. If one of the numbers $n - 1$, n, or $n + 1$ is divisible by 5, we are done. So we consider only the cases where $n = 5k + 2$ or $n = 5k + 3$. Refer to Exercise 11 of 1.1 for the remainder of the proof. ∎

EXERCISE 10. *Find all primes p such that $29p + 1$ is a square.*

SOLUTION. From the proof of Exercise 11, it follows that p can only be 31. ∎

EXERCISE 11. *The prime numbers p and q are called twin primes if $|p - q| = 2$. Let p and q be primes. Prove that $pq + 1$ is a square if and only if p and q are twin primes.*

SOLUTION.

EXERCISE 12. *Prove that if p and q are twin primes greater than 3, then $p + q$ is divisible by 12.*

SOLUTION. Without loss of generality, we assume $q = p + 2$ and $p > 3$. Since $p, p + 1, q$ are three consecutive numbers, one of them is divisible by 3 and $p + 1$ is divisible by 2. But p and q are primes greater than 3. It follows that $p + 1$ is also divisible by 3. Let $p + 1 = 6k$ for some $k \in \mathbb{Z}$. Then $p + q = 6k - 1 + 6k - 1 + 2 = 12k$. The proposition follows. ∎

EXERCISE 13. *Let m, n, and k be positive integers. Prove that*

$$v_p(mn) = v_p(m) + v_p(n) \qquad and \qquad v_p(m^k) = kv_p(m).$$

SOLUTION. The second relation readily follows from the first using induction. To prove the first we write the prime factorizations of m and n as follows:

$$m = p^{v_p(m)} \prod_{p_*} p_*^{v_{p_*}(m)} \qquad \text{and} \qquad n = p^{v_p(m)} \prod_{p_*} p_*^{v_{p_*}(m)}$$

where p_* are distinct primes different from p. Therefore, the product in each expansion does not involve p. Then mn has the prime factorization

$$mn = p^{v_p(m)+v_p(n)} \prod_{p_*} p_*^{v_{p_*}(mn)}.$$

We observe that $p^{v_p(m)+v_p(n)}$ but no higher power of p divides mn. By definition, it follows that $v_p(mn) = v_p(m) + v_p(n)$. ∎

EXERCISE 14. *Let d and m be nonzero integers. Prove that d divides m if and only if $v_p(d) \leq v_p(m)$ for all primes p.*

SOLUTION.

EXERCISE 15. *Let $m = \prod_{i=1}^{k} p_i^{r_i}$, where $p_1, \ldots, p_k$ are distinct primes, $k \geq 2$, and $r_i \geq 1$ for $i = 1, \ldots, k$. Let $m_i = mp_i^{-k_i}$ for $i = 1, \ldots, k$. Prove that $(m_1, \ldots, m_k) = 1$.*

SOLUTION.

EXERCISE 16. *Let a, b and c be positive integers. Prove that $(ab, c) = 1$ if and only if $(a, c) = (b, c) = 1$.*

SOLUTION.

EXERCISE 17. *Prove that if 6 divides m, then there exist integers b and c such that $m = bc$ and 6 divides neither b nor c.*

SOLUTION. From the prime factorization of m, we can construct two integers b and c such that $m = bc$, $v_2(m) = v_2(b)$ and $v_3(m) = v_3(c)$. That is, 3 does not appear in the prime factorization of b neither do 2 appear in the prime factorization c. Consequently, 6 divides neither b nor c. ∎

EXERCISE 18. *Prove the following statement or construct a counterexample: If d is composite and d divides m, then there exists integers b and c such that $m = bc$ and d divides neither b nor c.*

SOLUTION.

EXERCISE 19. *Let a and b be positive integers. Prove that $(a, bc) = (a, b)(a, c)$ for every positive integer c if and only if $(a, b) = 1$.*

SOLUTION.

EXERCISE 20. *Let $m_1, \ldots, m_k$ be pairwise relatively prime positive integers, and let d divide $m_1 \cdots m_k$. Prove that for each $i = 1, \ldots, k$ there exists a unique divisor d_i of m_i such that $d = d_1 \cdots d_k$.*

SOLUTION. Since d divides $m_1 \cdots m_k$ and $m_1, \ldots, m_k$ are pairwise relatively prime, every prime that divides d divides only one integer among $m_1, \ldots, m_k$. Let P be the set of distinct primes that divide d. We define a relation R on P as follows: pRq if and only if $p, q \in P$ and both p and q divide one m_i for $1 \leq i \leq k$. Clearly R is an equivalence relation and it partitions P into the pairwise disjoint sets $M_1, \ldots, M_k$ such that M_i is the set of all primes which divide both d and m_i for each $1 \leq i \leq k$. We define

$$d_i := \prod_{p}^{M_i} p^{v_p(d)}$$

for each $1 \leq i \leq k$ and $p \in M_i$. Clearly $d = d_1 \cdots d_k$. By construction, each d_i is unique. ∎

1.5   Euclid's Theorem and the Sieve of Erastosthenes

Exercises 1-4 can be solved using the sieve of Eratosthenes (although it might be long and tedious in some cases) and method of exhaustion (to exhaust each possible case).

EXERCISE 5. *Let a and n be positive integers. Prove that $a^n - 1$ is prime only if $a = 2$ and $n = p$ is prime. Primes of the form $M_p = 2^p - 1$ are called Mersenne primes. Compute the first five Mersenne primes.*

SOLUTION.

EXERCISE 6. *Let k be a positive integer. Prove that if $2^k + 1$ is prime, then $k = 2^n$. The integer*

$$F_n = 2^{2^n} + 1$$

is called the nth Fermat number. Primes of the form $2^{2^n} + 1$ are called Fermat primes. Show that F_n is prime for $n = 1, 2, 3, 4$.

SOLUTION.

EXERCISE 7. *Prove that F_5 is divisible by 641, and so F_5 is composite.*

SOLUTION. We see that $F_5 = 2^{2^5} - 1 = (2^{32} + 5^4 \cdot 2^{28}) - (5^4 \cdot 2^{28} - 1)$ and $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$. But we can write $2^{32} + 5^4 \cdot 2^{28} = 2^{28}(2^4 + 5^4)$ and $5^4 \cdot 2^{28} - 1 = (5^2 \cdot 2^{14} + 1)(5 \cdot 2^7 + 1)(5 \cdot 2^7 - 1)$. Therefore, 641 divides both $5^4 \cdot 2^{28} + 2^{32}$ and $5^4 \cdot 2^{28} - 1$. The proposition follows. ∎

EXERCISE 9. *Show that every prime number except 2 and 3 has the remainder of 1 or 5 when divided by 6. Prove that there are infinitely many prime numbers whose remainder is 5 when divided by 6.*

SOLUTION. Every integer is one and only one of the forms $6k$, $6k + 1$, $6k + 2$, $6k + 3$, $6k + 4$, or $6k + 5$ for some $k \in \mathbb{Z}$. Out of these, $6k$, $6k + 2$, and $6k + 4$ are divisible by 2 and cannot be prime. Similarly, $6k + 3$ is divisible by 3 and is not prime. Consequently, every prime > 3 is one of the forms: $6k + 1$ or $6k + 5$.

EXERCISE 10. *Prove that $\pi(n) \leq n/2$ for $n \geq 8$.*

SOLUTION.

1.6   A Linear Diophantine Equation

EXERCISE 1. *Prove that the equation*

$$3x_1 + 5x_2 = b$$

has a solution in integers for every integer b, and a solution in nonnegative integers for $b = 0, 3, 5, 6$ and all $b \geq 8$.

SOLUTION. Since $\gcd(3, 5) = 1$, the equation has a solution in integers for every $b \in \mathbb{Z}$. We see that $3 \cdot 0 + 5 \cdot 0 = 0$, $3 \cdot 1 + 5 \cdot 0 = 3$, $3 \cdot 0 + 5 \cdot 1 = 5$ and $3 \cdot 2 + 5 \cdot 0 = 6$. Also for a Frobenius linear diophantine equation, $G(3, 5) = (3 - 1)(5 - 1) = 8$. The proposition follows. ∎

EXERCISE 2. *Find all solutions in nonnegative integers x_1 and x_2 of the linear diophantine solution*

$$2x_1 + 7x_2 = 53.$$

SOLUTION. The following are all the combinations of (x_1, x_2) that satisfy the equation:

$$2 \cdot 23 + 7 \cdot 1 = 53, \qquad 2 \cdot 9 + 7 \cdot 5 = 53,$$
$$2 \cdot 16 + 7 \cdot 3 = 53, \qquad 2 \cdot 2 + 7 \cdot 7 = 53. \blacksquare$$

Exercise 3 may be solved similarly.

EXERCISE 4. *Let a_2 and a_2 be relatively prime positive integers. Let $N(a_1, a_2)$ denote the number of nonnegative integers that cannot be represented in the form*

$$a_1 x_1 + a_2 x_2$$

with x_1, x_2 nonnegative integers. Compute $N(3, 10)$ and $N(3, 10)/G(3, 10)$.

SOLUTION. For a Frobenius linear diophantine equation, $G(3, 10) = (3 - 1)(10 - 1) = 18$. Let $V(x_1, x_2) = 3x_1 + 10x_2$. All the possible combinations (x_1, x_2) of nonnegative integers x_1, x_2 such that $V < 18$ are given by the following equations.

$$V(0,0) = 0, \qquad V(1,0) = 3, \qquad V(2,0) = 6,$$
$$V(3,0) = 9, \qquad V(4,0) = 12, \qquad V(5,0) = 15,$$
$$V(0,1) = 10, \qquad V(1,1) = 13, \qquad V(2,1) = 16.$$

Since $G(3, 10) = 18$, it follows that the only nonnegative integers that cannot to represented in the form $3x_1 + 10x_2$ are 1, 2, 4, 5, 7, 8, 11, 14, and 17. Therefore, $N(3, 10) = 9$ and $N(3, 10)/G(3, 10) = 1/2$. $\blacksquare$

Exercise 5 may be solved similarly.

EXERCISE 6. *Find all nonnegative integers that cannot be represented by the form*

$$3x_1 + 10x_2 + 14x_3$$

with x_1, x_2, x_3 nonnegative integers. Compute $G(3, 10, 14)$.

SOLUTION. Let $V(x_1, x_2, x_3) = 3x_1 + 10x_2 + 14x_3$. We see that $(3-1) \cdot 14 \cdot 10 = 280$. Therefore, every $b \geq 280$ can be represented by the form $V(x_1, x_2, x_3)$, and we need only check for those (x_1, x_2, x_3) such that $V(x_1, x_2, x_3) < 280$. As in Exercise 4, we make a table of all possible values of $V(x_1, x_2, x_3)$ avoiding, of course, multiples of 3, 10, 14, 30, 70, and 210 and find that the only nonnegative integers that cannot be represented in the form $3x_1 + 10x_2 + 10x_3$ are $\{1, 2, 4, 5, 7, 8, 11\}$. It follows that $G(3, 10, 14) = 12$. $\blacksquare$

Exercise 8 is similar to Exercise 2.

EXERCISE 9. *Find all solutions in integers x_1, x_2 and x_3 of the system of linear diophantine equations*

$$3x_1 + 5x_2 + 7x_3 = 560, \qquad 9x_1 + 25x_2 + 49x_3 = 2920.$$

SOLUTION. Putting $x_3 = k$, we reduce the given system to a linear system in two unknowns:

$$3x_1 + 5x_2 = 560 - 7k,$$
$$9x_1 + 25x_2 = 2920 - 49k,$$

whose solutions, by Cramer's rule, are given by

$$x_1 = \frac{7}{3}k - 20; \qquad x_2 = 124 - \frac{14}{5}k.$$

Since we are interested only in nonnegative integer solutions, we look into the cases where k is divisible by both 3 and 5 such that x_1 and x_2 are both nonnegative. It is easy to see that the only solution is $(15, 82, 15)$. ∎

2 Congruences

2.1 The Ring of Congruence Classes

Exercises 1-4 are simple computations of modulo arithmetic. Exercise 5 is a special case of Exercise 6, which we will now solve.

EXERCISE 6. *Let m be an odd positive integer. Prove that every integer is congruent modulo m to one of the even integers 0, 2, 4, 6, ..., $2m - 2$.*

SOLUTION. Let $X = \{0, 1, 2, \ldots, m - 1\}$ be the complete set of residues modulo m. Let $Y = \{0, 2, 4, \ldots, 2m - 2\}$. Let $f : X \to Y$ be a map defined by

$$f(x) = \begin{cases} x & \text{if } x \text{ is even} \\ x + m & \text{otherwise.} \end{cases}$$

This function maps every integer to its congruent modulo m in the set Y. ∎

Exercise 7 is a special case of Exercise 8, which we will now solve.

EXERCISE 8. *Let $m = 2q + 1$ be an odd positive integer. Prove that every integer is congruent modulo m to a unique integer r such that $-q \leq r \leq q$.*

SOLUTION. As in Exercise 6, we only need to find the correct map. Let $X = \{0, 1, 2, \ldots, 2q\}$ be the complete set of residues modulo $2q + 1$. Let $Y = \{-q, -q + 1, \ldots, q - 1, q\}$. Then the function $f : X \to Y$ defined by

$$f(x) = \begin{cases} x & \text{if } x \leq q \\ x - (2q + 1) & \text{if } x \geq q. \end{cases}$$

maps every integer to its congruent modulo $2q + 1$ in the set Y. The uniqueness follows from the fact that f is a bijection. ∎

EXERCISE 9. *Let $m = 2q$ be an even positive integer. Prove that every integer is congruent modulo m to a unique integer r such that $-(q - 1) \leq r \leq q$.*

14

SOLUTION. Let $X = \{0, 1, 2, \ldots, 2q - 1\}$ be the complete set of residues modulo $2q$. Let $Y = \{-(q-1), -q+2, \ldots, q-1, q\}$. Then the function $f : X \to Y$ defined by

$$f(x) = \begin{cases} x & \text{if } x \leq q \\ x - 2q & \text{if } x \geq q. \end{cases}$$

maps every integer to its congruent modulo $2q$ in the set Y. The uniqueness follows from the fact that f is a bijection. ∎

EXERCISE 10. *Prove that $a^3 \equiv a(\mod 6)$ for every integer a.*

SOLUTION. It suffices to prove that $a^3 - a$ is divisible by 6, which we already did in Exercise 10 of 1.1. ∎

EXERCISE 11. *Prove that $a^4 \equiv 1(\mod 5)$ for every integer a that is not divisible by 5.*

SOLUTION. It suffices to prove that $a^4 - 1$, that is, $(a^2 + 1)(a + 1)(a - 1)$ is divisible by 5. If either $a + 1$ or $a - 1$ is divisible by 5 then we are done. Excluding these cases, a can only be one of the forms: $5k + 2$ or $5k + 3$ for some $k \in \mathbb{Z}$. Suppose $a = 5k + 2$. Then (by expansion or using binomial theorem) $a^4 - 1 = 5^4 a^4 + 4 \cdot 5^3 a^3 \cdot 2 + 6 \cdot 5^2 a^2 \cdot 2^2 + 4 \cdot 5a \cdot 2^3 + 15$, which is divisible by 5. The other case of a of the form $5k + 3$ is proved similarly. ∎

Exercise 12 is exactly the same as Exercise 9 of 1.1.

2.2 Linear Congruences

Exercises 1-2 are similar and as such, we solve only Exercise 2.

EXERCISE 2. *Find all solutions of the congruence $12x \equiv 3(\mod 45)$.*

SOLUTION. On division by 3, we may reduce the problem to finding the solutions of the congruence $4x \equiv 1(\mod 15)$. Since $\gcd(15, 4) = 1$, this equation has exactly one solution which is $x \equiv 4(\mod 15)$. The complete set of solutions that are pairwise incongruent modulo 45 is $\{4, 19, 34\}$. ∎

EXERCISE 3. *Find all solutions of the congruence $28x \equiv 35(\mod 42)$.*

SOLUTION. On division by 7, we may reduce the problem to finding the solutions of $4x \equiv 5(\mod 6)$. Since $\gcd(4, 6) = 2$ and 2 does not divide 5, the given equation has no solutions. ∎

2.3 The Euler Phi Function

Exercise 1 is a simple computation problem using the Euler totient function (may be solved by writing down the canonical decomposition of 6993 and using the fact that the Euler totient function is multiplicative).

EXERCISE 2. *Represent the congruence classes modulo 12 in the form $3a + 4b$ with $0 \leq a \leq 3$ and $0 \leq b \leq 2$.*

SOLUTION. The congruence classes modulo 12 may be represented as linear combinations of 3 and 4 as follows:

$$0 \equiv 0 \cdot 3 + 0 \cdot 4 \mod 12 \qquad\qquad 6 \equiv 2 \cdot 3 + 0 \cdot 4 \mod 12$$
$$1 \equiv 3 \cdot 3 + 1 \cdot 4 \mod 12 \qquad\qquad 7 \equiv 1 \cdot 3 + 1 \cdot 4 \mod 12$$
$$2 \equiv 3 \cdot 3 + 2 \cdot 4 \mod 12 \qquad\qquad 8 \equiv 0 \cdot 3 + 2 \cdot 4 \mod 12$$
$$3 \equiv 1 \cdot 3 + 0 \cdot 4 \mod 12 \qquad\qquad 9 \equiv 3 \cdot 3 + 0 \cdot 4 \mod 12$$
$$4 \equiv 0 \cdot 3 + 1 \cdot 4 \mod 12 \qquad\qquad 10 \equiv 2 \cdot 3 + 1 \cdot 4 \mod 12$$
$$5 \equiv 3 \cdot 3 + 2 \cdot 4 \mod 12 \qquad\qquad 11 \equiv 1 \cdot 3 + 2 \cdot 4 \mod 12$$

Exercise 3 is a simple verification.

EXERCISE 4. *Prove that $\varphi(m)$ is even for all $m \geq 3$.*

SOLUTION. The value $\varphi(m)$ equals the number of positive integers less than m which are relatively prime to m. Let $m \geq 3$. Let $1 \leq k \leq m$ be such that $\gcd(k, m) = 1$. Then $\gcd(m - k, m) = 1$ such that all positive integers less than m which are relatively prime to m can be written in pairs $\{k, m - k\}$. Therefore, $\varphi(m)$ is even. ∎

EXERCISE 5. *Prove that $\varphi(m^k) = m^{k-1}\varphi(m)$ for all positive integers m and k.*

SOLUTION. Using the formula for φ, we have

$$\varphi(m^k) = m^k \prod_{p \mid m^k} \left(1 - \frac{1}{p}\right) = m^{k-1} \cdot m \prod_{p \mid m} \left(1 - \frac{1}{p}\right) = m^{k-1}\varphi(m),$$

where we have used the fact that m^k and m would have same prime divisors. ∎

EXERCISE 6. *Prove that m is prime if and only if $\varphi(m) = m - 1$.*

SOLUTION. Suppose m is prime. Then $\gcd(k, m) = 1$ for all $1 \leq k \leq m - 1$ (otherwise k and m would have a common factor greater than 1 and m would not be prime) so that $\varphi(m) = m - 1$. Conversely suppose $\varphi(m) = m - 1$. This implies that no positive integer less than m divides m. Evidently m is prime. ∎

EXERCISE 7. *Prove that $\varphi(m) = \varphi(2m)$ if and only if m is odd.*

SOLUTION. Suppose m is odd. Then $\gcd(m, 2) = 1$. Since φ is multiplicative, it follows that $\varphi(2m) = \varphi(2) \cdot \varphi(m) = \varphi(m)$. Conversely, suppose $\varphi(2m) = \varphi(m)$.

EXERCISE 8. *Prove that if m divides n, then $\varphi(m)$ divides $\varphi(n)$.*

SOLUTION. This becomes obvious once we write down the expressions

$$\varphi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right); \qquad \varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Since $m \mid n$, every prime that divides m also divides n. That is, every term in the product $\varphi(m)$ is in the product $\varphi(n)$. Evidently $\varphi(m)$ divides $\varphi(n)$. ∎

EXERCISE 9. *Find all positive integers n such that $\varphi(n)$ is not divisible by 4.*

SOLUTION.

EXERCISE 10. *Find all positive integers n such that $\varphi(5n) = 5\varphi(n)$.*

SOLUTION. The relation is true for all n which are not divisible by 5. ∎

2.4 Chinese Remainder Theorem

EXERCISE 1. *Find all solutions of the system of congruences*

$$x \equiv 4 \mod 5; \qquad x \equiv 5 \mod 6.$$

SOLUTION. Since $\gcd(5, 6) = 1$ and $5 \equiv 4 \mod 1$, the system has a solution. From the first congruence, we have $x = 4 + 5u$. Using this in the second congruence, we have $5u \equiv 1 \mod 6$ which has the solution $u \equiv 5 \mod 6$. All solutions of the system is then given by $4 + 5(5 + 6v) = 29 + 30v$, that is, $29 + 30\mathbb{Z}$. ∎

Exercises 2-3 are solved similarly.

EXERCISE 4. *Find all solutions of the system of congruences*

$$2x \equiv 1 \mod 5; \qquad 3x \equiv 4 \mod 7.$$

SOLUTION.

EXERCISE 5. *Find all integers that have a remainder of 1 when divided by 3, 5 and 7.*

SOLUTION. We simply need to find all solutions to the following system of congruences:

$$x \equiv 1 \mod 3; \qquad x \equiv 1 \mod 5; \qquad x \equiv 1 \mod 7.$$

From the first two congruences, we have $3u \equiv 0 \mod 5$ whose solution is $u \equiv 0 \mod 5$. Therefore the solution to the first two congruences is $1 + 15v$. Continuing with the third congruence, we find that the solutions are indeed $1 + 105\mathbb{Z}$. ∎

EXERCISE 6. *Find all integers that have a remainder of 2 when divided by 4 and that have a remainder of 3 when divided by 5.*

SOLUTION. We simply need to find all solutions to the following system of congruences:

$$x \equiv 2 \mod 4; \qquad x \equiv 3 \mod 5.$$

As before, we find the general solution to be $18 + 20\mathbb{Z}$. ∎

EXERCISE 7. *Find all solutions of the congruence*

$$f(x) = 5x^3 - 93 \equiv 0 \mod 231.$$

SOLUTION. Since $231 = 3 \cdot 7 \cdot 11$, it suffices to solve the congruences

$$5x^3 - 93 \equiv 0 \mod 3; \qquad 5x^3 - 93 \equiv 0 \mod 7; \qquad 5x^3 - 93 \equiv 0 \mod 11.$$

Or equivalently,

$$5x^3 \equiv 0 \mod 3; \qquad 5x^3 - 2 \equiv 0 \mod 7; \qquad 5x^3 + 6 \equiv 0 \mod 11.$$

These congruences have solutions

$$f(0) \equiv 0 \mod 3; \qquad f(3) \equiv 0 \mod 7; \qquad f(1) \equiv 0 \mod 11.$$

By the Chinese remainder theorem, there exists an integer a such that

$$a \equiv 0 \mod 3; \qquad a \equiv 3 \mod 7; \qquad a \equiv 1 \mod 11.$$

Solving these congruences, we obtain $a \equiv 45 \mod 231$. We may check that $f(45) =$

2.5 Euler's Theorem and Fermat's Theorem

EXERCISE 1. *Prove that* $3^{512} \equiv 1 \mod 1024$.

SOLUTION. The Euler totient function yields $\varphi(1024) =$

EXERCISE 2. *Find the remainder when* 7^{51} *is divided by* 144.

SOLUTION. Let $x = 7^{51} \mod 144$. We observe that $7^3 \mod 144 = 55 \mod 144$ so that $x = 55^{17} \mod 144$. We again observe that $55^2 \mod 144 = 1 \mod 144$ rendering $x = 55 \mod 144$. ∎

Exercise 3 is solved similarly.

EXERCISE 4. *Compute the order of* 2 *with respect to the prime moduli* 3, 5, 7, 11, 13, 17 *and* 19.

SOLUTION. We observe that 2 is relatively prime to each of these given primes. Therefore the orders are respectively 3, 5, 7, 11, 13, 17 and 19. ∎

EXERCISE 5. *Compute the order of* 10 *with respect to the modulus* 7.

SOLUTION. Since $10 \equiv 3 \mod 7$ and $\gcd(3, 7) = 1$, the order is $\varphi(7)$, that is 6. ∎

EXERCISE 6. *Let* r_i *denote the least nonnegative residue of* $10^i \mod 7$. *Compute* r_i *for* $i = 1, \ldots, 6$. *Compute the decimal expansion of the fraction* 1/7 *without using a calculator. Can you find where the numbers* $r_1, \ldots, r_6$ *appear in the process of dividing* 7 *into* 1?

SOLUTION. We compute $r_1 \equiv 3 \mod 7$, $r_2 \equiv 2 \mod 7$, $r_3 \equiv 6 \mod 7$, $r_4 \equiv 4 \mod 7$, $r_5 \equiv 5 \mod 7$, $r_6 \equiv 1 \mod 7$. The decimal expansion of 1/7 is .142857...

EXERCISE 7. *Compute the order of* 10 *modulo* 13. *Compute the period of the fraction* 1/13.

SOLUTION. Since $\gcd(10, 13) = 1$, the order is $\varphi(13)$, that is, 6. The period of the fraction 1/13 is 6. ∎

EXERCISE 8. *Let* p *be a prime and* a *an integer not divisible by* p. *Prove that if* $a^{2^n} \equiv -1 \mod p$, *then* a *has order* $2^{n+1} \mod p$.

SOLUTION. On multiplying the congruence by itself, we have $a^{2^{n+1}} \equiv 1 \mod p$. We observe that 2^{n+1} has only 2 as its prime factor. It is easy to see that there is no k with $1 \le k < 2^{n+1}$ such that $a^k \equiv 1 \mod p$. Therefore, a has order $2^{n+1} \mod p$. ■

3 Primitive Roots and Quadratic Reciprocity

3.1 Polynomials and Primitive Roots

EXERCISE 1. *Find a primitive root modulo* 23.

SOLUTION. 23 is a prime and $\varphi(22) = 10$. Therefore, there are 10 primitive roots modulo 23. 2 is such one primitive root modulo 23. ■

Exercise 2 may be solved similarly.

EXERCISE 3. *Prove that* 2 *is a primitive root modulo* 101.

SOLUTION. The Euler totient function yields $\varphi(101) = 100$. Repeatedly computing $2^i \mod 101$ for $1 \le i \le 100$, we find that 2 has order 100 $\mod 101$. Hence the result. ■

EXERCISE 4. *Compute* $\mathrm{ind}_2(27)$ *modulo* 101.

SOLUTION. In Exercise 3 we proved that 2 is a primitive root of 101. Thus, $27 \equiv 2^k \mod 101$ has a unique solution satisfying $0 \le k \le 99$. By computation, we find $\mathrm{ind}_2(27) = 7$. ■

Exercise 5 may be solved similarly.

EXERCISE 6. *What is the order of* 3 *modulo* 101? *Is* 3 *a primitive root modulo* 101?

SOLUTION. By successive computation of $3^i \mod 101$ for $i \ge 1$ we find that $3^{100} \equiv 1 \mod 101$ and there is no $k \le 100$ satisfying $3^k \equiv 1 \mod 101$. That is, the order of 3 $\mod 101$ is 100. But $\varphi(101) = 100$. Therefore, 3 is a primitive root modulo 101. ■

Exercise 7 is similar to Exercise 3.

EXERCISE 8. *Find all solutions of the congruence* $2^x \equiv 22 \mod 53$.

SOLUTION. In Exercise 7, we prove that 2 is a primitive root modulo 53. We observe that $2^7 \equiv 22 \mod 53$.

3.2 Primitive Roots to Composite Moduli

EXERCISE 1. *Find an integer* g *that is a primitive root moduli* 5^k *for all* $k \ge 1$. *Find a primitive root modulo* 10. *Find a primitive root modulo* 50.

SOLUTION. Since $\mathrm{ord}_5(2) = 4 = \varphi(5)$, 2 is a primitive root of 5. We observe that the highest power of 3 which divides $2^4 - 1$ is 3. Further, $\varphi(5^k) = 4 \cdot 5^{k-1}$. By Theorem 3.6, it follows that 2 is a primitive root modulo 5^k for all $k \ge 1$. Since $10 = 2 \cdot 5$ and $2 + 5 = 7$ is odd, by

Theorem 3.7, it follows that 7 is a primitive root modulo 10. Finally, $50 = 2 \cdot 5^2$ and 2 is a primitive root modulo 25. Since $2 + 5^2 = 27$ is odd, 27 is a primitive root modulo 50. ∎

EXERCISE 2. *For $k \geq 1$, let e_k be the order of 5 modulo 3^k. Prove that*

$$e_k = 2 \cdot 3^{k-1}.$$

SOLUTION. We begin by observing that 5 is a primitive root of 3 (because $5 \equiv 2 \mod 3$, $5^2 \equiv 1 \mod 3$ and $\varphi(3) = 2$). Since the highest power of 3 which divides $5^2 - 1$ is 3 and $\varphi(3^k) = 2 \cdot 3^{k-1}$, by Theorem 3.6, it follows that 5 is a primitive root of 3^k for all $k \geq 1$. Therefore, $e_k = \varphi(3^k) = 2 \cdot 3^{k-1}$. ∎

EXERCISE 3. *Prove that p divides the binomial coefficient $\binom{p}{i}$ for $i = 1, 2, \ldots, p-1$.*

SOLUTION.

EXERCISE 4. *Prove that if g is a primitive root modulo p^2, then g is a primitive root modulo p^k for all $k \geq 2$.*

SOLUTION. If we can prove that g is a primitive root modulo p, then (by Theorem 3.7) we are done.

EXERCISE 7. *Use Exercise 6 to prove that the exponential congruence*

$$9^k \equiv 1 \mod 7^k$$

has no solutions.

SOLUTION. We see that $\mathrm{ord}_7(9) = 3$ and the highest power of 7 which divides $9^3 - 1$ is 7. Suppose the given congruence has solutions. Then by Exercise 6, we have

$$\frac{7^k}{k} < \frac{9^3}{3} = 243 \implies 7^k < 243k,$$

which cannot hold for $k \geq 4$. It is easy to check that it has no solutions for $k = 1, 2, 3$ as well. The proposition follows. ∎

3.3 Power Residues

Exercise 1 has been solved in the text.

EXERCISE 2. *Find all solutions of the congruence $x^3 \equiv 8 \mod 19$.*

SOLUTION. In Exercise 1, we saw that 8 is a cubic residue modulo 19. Also, $\gcd(3, 18) = 6$. By Theorem 3.11, it follows that the congruence has exactly 6 solutions that are pairwise incongruent modulo 19.

EXERCISE 3. *Define the map $f : (\mathbb{Z}/19\mathbb{Z})^\times \to (\mathbb{Z}/19\mathbb{Z})^\times$ by $f(x + 19\mathbb{Z}) = x^3 + 19\mathbb{Z}$. Prove that f is a homomorphism of the multiplicative group $(\mathbb{Z}/19\mathbb{Z})^\times$, and compute its kernel.*

SOLUTION. Homomorphism follows from the fact that $f(xy) = (xy)^3 + 19\mathbb{Z} = (x^3 + 19\mathbb{Z})(y^3 + 19\mathbb{Z}) = f(x)f(y)$ for all $x, y \in \mathbb{Z}/19\mathbb{Z}$. Any $k \in \ker(f)$ satisfies the congruence

$$k^3 \equiv 1 \mod 19.$$

20

It is checked that the solutions are $1 + 19\mathbb{Z}$, $7 + 19\mathbb{Z}$, and $11 + 19\mathbb{Z}$. These are the elements of $\ker(f)$. ∎

EXERCISE 6. *Define the map $f : (\mathbb{Z}/23\mathbb{Z})^\times \to (\mathbb{Z}/23\mathbb{Z})^\times$ by $f(x + 23\mathbb{Z}) = x^3 + 23\mathbb{Z}$. Prove that f is an isomorphism of the multiplicative group $(\mathbb{Z}/23\mathbb{Z})^\times$, that is, prove that f is a homomorphism that is one-one and onto.*

3.4   Quadratic Residues

EXERCISE 1. *Find all solutions of the congruences $x^2 \equiv 2 \mod 47$ and $x^2 \equiv 2 \mod 53$.*

SOLUTION. Since $\left(\frac{2}{47}\right) = 2^{(47-1)/2} = 1$, the congruence has a solution. Since it is a quadratic equation modulo a prime, there are two solutions (or square roots of 2 modulo 47). By computation, we find that $7^2 \equiv 2 \mod 47$ and $40^2 \equiv 2 \mod 47$. Therefore, the solutions are $7 + 47\mathbb{Z}$ and $40 + 47\mathbb{Z}$. The other congruence is solved similarly. ∎

EXERCISE 2. *Prove that $S = \{3, 4, 5, 9, 10\}$ is a Gaussian set modulo 11. Apply Gauss's lemma to this set to compute the Legendre symbols $\left(\frac{3}{11}\right)$ and $\left(\frac{7}{11}\right)$.*

SOLUTION. We observe that $-10 \equiv 1 \mod 11$, $-9 \equiv 2 \mod 11$, $-5 \equiv 6 \mod 11$, $-4 \equiv 7 \mod 11$, and $-3 \equiv 8 \mod 11$. Since $S \cup -S = \{-10, -9, 3, 4, 5, -5, -4, -3, 9, 10\}$ and $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ is a complete set of residues modulo 11, it follows that S is a Gaussian set. We now compute the following:

$$
\begin{array}{ll}
3 \cdot 3 \equiv 9 \mod 11, & 7 \cdot 3 \equiv 10 \mod 11, \\
3 \cdot 4 \equiv (-1)10 \mod 11, & 7 \cdot 4 \equiv (-1)5 \mod 11, \\
3 \cdot 5 \equiv 4 \mod 11, & 7 \cdot 5 \equiv 3 \mod 11, \\
3 \cdot 9 \equiv 5 \mod 11, & 7 \cdot 9 \equiv (-1)3 \mod 11, \\
3 \cdot 10 \equiv (-1)3 \mod 11, & 7 \cdot 10 \equiv 4 \mod 11.
\end{array}
$$

From the above table, it follows that $\left(\frac{3}{11}\right) = 1$ and $\left(\frac{7}{11}\right) = 1$. ∎

EXERCISE 3. *Let p be an odd prime. Prove that $\{2, 4, 6, \ldots, p-1\}$ is a Gaussian set modulo p.*

SOLUTION. Let $S = \{2, 4, 6, \ldots, p-1\}$. Then $-S = \{-(p-1), -(p-3), \ldots, -2\}$. We observe that $-(p-1) \equiv 1 \mod p$, $-(p-3) \equiv 3 \mod p$, $\ldots$, $-2 \equiv p-2 \mod p$. Clearly $S \cup -S = \{1, 2, \ldots, p-1\}$ is a complete set of residues modulo p. The proposition follows. ∎

EXERCISE 4. *Use Theorem 3.14 and Theorem 3.16 to find all primes p for which -2 is a quadratic residue.*

SOLUTION. By Theorem 3.14 and Theorem 3.16, we have

$$
\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p^2-1)/8} = (-1)^{\frac{1}{8}(p-1)(p+5)}.
$$

EXERCISE 8. *Let p be an odd prime. Prove that the Legendre symbol is a homomorphism from the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ into $\{\pm 1\}$. What is the kernel of this homomorphism?*

SOLUTION. For any $a \in (\mathbb{Z}/p\mathbb{Z})^{\times}$, p does not divide a. That is, the Legendre symbol $\left(\frac{a}{p}\right) = \pm 1$ for all $a \in (\mathbb{Z}/p\mathbb{Z})^{\times}$. Then the homomorphism follows from the fact that the Legendre symbol is completely multiplicative arithmetic function. That is,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

for all $a, b \in (\mathbb{Z}/p\mathbb{Z})^{\times}$. The kernel is the set of all $a \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ which are quadratic residue modulo p. ■

3.5 Quadratic Reciprocity Law

EXERCISE 2. *Use quadratic reciprocity to compute* $\left(\frac{7}{43}\right)$. *Find an integer x such that $x^2 \equiv 7$* mod 43.

SOLUTION. We observe that $7 \equiv 3 \mod 4$, and $43 \equiv 3 \mod 4$. By quadratic reciprocity law,

$$\left(\frac{7}{43}\right) = -\left(\frac{43}{7}\right) = -\left(\frac{1}{7}\right) = -1.$$

Therefore, there is no integer x such that $x^2 \equiv 7 \mod 43$. ■

Exercise 3 is similar to Exercise 2.

EXERCISE 6. *Use quadratic reciprocity to find all primes p for which 3 is a quadratic residue.*

SOLUTION. If $p \equiv 1 \mod 4$, by quadratic reciprocity, we have

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 3, \\ -1 & \text{if } p \equiv 2 \mod 3. \end{cases}$$

If $p \equiv 3 \mod 4$, by quadratic reciprocity, we have

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 2 \mod 3, \\ -1 & \text{if } p \equiv 1 \mod 3. \end{cases} ∎$$