Solutions to Nathanson's
Elementary Methods in Number Theory

H. Ronald

These are my solutions to the first three chapters of the Nathanson's text (mentioned in the cover title). At the moment, not all problems are solved. Similar problems are omitted. Some simple computational problems are also omitted. A few solutions are incomplete (I will complete them soon) and they can be identified with their lack of □ symbol. I have discovered that a few solutions have errors (I will correct them soon). I have thoroughly enjoyed solving all these problems on my own.

The latest version of this text can be found at ⟨github.com/ronhuidrom/nathanson-number-theory/blob/main/NathansonSolutions.pdf⟩ — I update it everyday as I keep adding more solutions (or correcting errors).

Ronald

Contents

1 Divisibility and Primes

1.1 Division Algorithm

Exercises 1-5 are straightforward (use prime factorization and division algorithm). 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.*

Proof. 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.*

Proof. 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.*

Proof. 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 $-d/2 < r' \leq d/2$.*

Proof. Let S be the set of integers of the form $a - dx$ with $x \in \mathbb{Z}$. We choose $r' = a - dx$ such that $-d/2 < a - dx \leq d/2$. It is possible to choose such an r' because $a - dx$ is an arithmetic progression with common difference d, and $|d/2 - (-d/2)| = d$. Then we set $q' = x$ so that $a = dq' + r'$. To prove uniqueness, we assume $a = dq_1 + r_1$ with $-d/2 < r_1 \leq d/2$. Since $-d/2 < r_1, r' \leq d/2$, and $a = dq_1 + r_1 = dq' + r'$, it follows that

$$|r_1 - r'| \leq d - 1, \qquad \text{and} \qquad d(q_1 - q') = r' - r_1.$$

If $q_1 \neq q'$, then

$$|q_1 - q'| \geq 1, \qquad \text{and} \qquad d \leq d|q_1 - q'| = |r' - r_1| \leq d - 1,$$

which is absurd. It follows that $q_1 = q'$ and $r_1 = r'$. □

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 $k!$.*

Proof. Any k consecutive integers are of the form $n, n-1, \ldots, n-(k-1)$. Their product can be written as

$$\frac{n(n-1)\cdots(n-k+1)(n-k)(n-k-1)\cdots 2\cdot 1}{(n-k)!} = \frac{n!}{(n-k)!}.$$

To prove that this product is divisible by $k!$, it suffices to prove that $n!/k!(n-k)!$, that is, $\binom{n}{k}$ is an integer. We prove this by using induction on n. The base case of $n=1$ is easily verified. Suppose the proposition holds for some $n \in \mathbb{Z}, n > 1$. By Exercise 20,

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1},$$

where both terms on the right side are integers (by induction hypothesis). Therefore, the term on the left side is an integer. The proposition follows. □

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.*

Proof. Any strictly increasing sequence of positive integers is unbounded. Thus, given any positive integer n, there exists $k \in \mathbb{Z}, k \geq 0$ such that $m_k \leq n < m_{k+1}$. For $k \geq 0$, let $P(k)$ be the statement that every integer in the interval $m_k \leq n < m_{k+1}$ has a unique representation in the form $\sum_{i=0}^{\infty} a_i m_i$, 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. Clearly $P(0)$ holds since $n = a_0$ is the unique representation if $1 \leq n \leq m_1$. Let $k \geq 1$ and suppose the statements $P(0)$, $P(1)$, $\ldots, P(k-1)$ hold. We shall prove $P(k)$. Let $m_k \leq n \leq m_{k+1}$. Then, by division algorithm,

$$n = a_k m_k + r, \qquad \text{where } 0 \leq r \leq m_k.$$

The remainder of the proof resembles the proof of unique m-acidic representation of an integer n given in the textbook. □

Exercise 23. *Prove that every positive integer n can be represented uniquely in the form*

$$n = \sum_{k=0}^{\infty} a_k k!$$

where $0 \leq a_k \leq k$.

Proof. We observe that $1!, 2!, 3!, \ldots$ is a strictly increasing sequence of positive integers satisfying the conditions of Exercise 22 and so, it reduces to Exercise 22. □

Exercise 24. *Prove that every positive integer n can be uniquely represented in the form*

$$n = b_0 + b_1 3 + b_2 3^2 + \cdots + b_{k-1} 3^{k-1} + 3^k,$$

where $b_i \in \{0, 1, -1\}$ for $i = 0, 1, 2, \ldots, k-1$.

Proof. We observe that $1, 3, 3^2, \ldots$ is a strictly increasing sequence of positive integers satisfying the conditions of Exercise 22 and so, it reduces to Exercise 22. □

Exercise 25. *Let $\mathbb{N}^k$ denote the set of all k-tuples of positive integers. We define the lexicographic order on $\mathbb{N}^k$ as follows: For $(a_1, \dots, a_k), (b_1, \dots, b_k) \in \mathbb{N}^k$, we write*

$$(a_1, \dots, a_k) \preceq (b_1, \dots, b_k)$$

if either $a_i = b_i$ for all $i = 1, \dots, k$, or there exists an integer j such that $a_i = b_i$ for $i < j$ and $a_j < b_j$. Prove that

(a) *The relation $\preceq$ is reflexive in the sense that if $(a_1, \dots, a_k) \preceq (b_1, \dots, b_k)$ and $(b_1, \dots, b_k) \preceq (a_1, \dots, a_k)$, then $(a_1, \dots, a_k) = (b_1, \dots, b_k)$.*

(b) *The relation is transitive in the sense that if $(a_1, \dots, a_k) \preceq (b_1, \dots, b_k)$ and $(b_1, \dots, b_k) \preceq (c_1, \dots, c_k)$, then $(a_1, \dots, a_k) \preceq (c_1, \dots, c_k)$.*

(c) *The relation is total in the sense that if $(a_1, \dots, a_k), (b_1, \dots, b_k) \in \mathbb{N}^k$, then $(a_1, \dots, a_k) \preceq (b_1, \dots, b_k)$ or $(b_1, \dots, b_k) \preceq (a_1, \dots, a_k)$.*

A relation that is reflexive and transitive is called a partial order. A partial order that is total is called a total order. Thus, the lexicographic order is a total order on the set of k-tuples of positive integers.

Proof. For the proofs, we shall use the well-ordering of natural numbers.

(a) Suppose $(a_1, \dots, a_k) \preceq (b_1, \dots, b_k)$ and $(b_1, \dots, b_k) \preceq (a_1, \dots, a_k)$. Then $a_1 \leq b_1$ and $b_1 \leq a_1$, so that $a_1 = b_1$. Since $a_1 = b_1$, we must have $a_2 \leq b_2$, and $b_2 \leq a_2$, so that $a_2 = b_2$ and so on. It follows that $(a_1, \dots, a_k) = (b_1, \dots, b_k)$.

(b) Suppose $(a_1, \dots, a_k) \preceq (b_1, \dots, b_k)$ and $(b_1, \dots, b_k) \preceq (c_1, \dots, c_k)$. Then there exists r with $1 \leq r \leq k$ and s with $1 \leq s \leq k$ such that $a_r < b_r$, $a_i = b_i$ for all $1 \leq i < r$, and $b_s < c_s$, $b_j = c_j$ for all $1 \leq j < s$. Two cases are possible: either $r \leq s$ or $s < r$. Suppose $r \leq s$. Then $a_r < c_r$, $a_i = c_i$ for all $1 \leq i < r$, so that $(a_1, \dots, a_k) \preceq (c_1, \dots, c_k)$. For the case when $s < r$, we have $a_s < c_s$, $a_i = c_i$ for all $1 \leq i < s$, so that $(a_1, \dots, a_k) \preceq (c_1, \dots, c_k)$.

(c) Suppose $(a_1, \dots, a_k), (b_1, \dots, b_k) \in \mathbb{N}^k$. We assume that $a_i \neq b_i$ for some $1 \leq i \leq n$, otherwise $(a_1, \dots, a_k) = (b_1, \dots, b_k)$ so that $(a_1, \dots, a_k) \preceq (b_1, \dots, b_k)$ and $(b_1, \dots, b_k) \preceq (a_1, \dots, a_k)$. Then we may assume that i is the smallest positive integer such that $a_i \neq b_i$. Then either $a_i < b_i$ or $b_i < a_i$ according to which $(a_1, \dots, a_k) \preceq (b_1, \dots, b_k)$ or $(b_1, \dots, b_k) \preceq (a_1, \dots, a_k)$. □

Exercise 26. *Prove that $\mathbb{N}^k$ with the lexicographic order satisfies the following minimum principle: Every nonempty set of k-tuples of positive integers contain a smallest element.*

Proof. Let S be any nonempty set of k-tuples of positive integers. We represent elements of S by a_i and we shall use the notation: $a_i := (a_{i1}, \dots, a_{ik})$. If $|S| = 1$, we are done. Let $|S| = n \neq 1$. Then we define a set $S_1 \subset S$ which contains all $a_i \in S$ with the smallest 1st coordinate (a_{i1}) among elements of S. The set S_1 is well-defined since the 1st coordinates are natural numbers and the set $\mathbb{N}$ is well-ordered (any nonempty subset of $\mathbb{N}$ has a least element). Thus, all elements $a_i \in S_1$ have the same 1st coordinate. In the same way, we define the set $S_j \subset S_{j-1}$ which contains all $a_i \in S_{j-1}$ with the smallest jth coordinate (a_{ij}) among elements of S_{j-1}. Clearly S_j is well-defined (use the same arguments as above). Now, we look at S_k.

By our construction, if $a_j \in S_k$, then $a_j \preceq a_i$ for all $a_i \in S$, so that a_j is the smallest element in S. □

1.2 Greatest Common Divisors

Exercises 1-2 are straightforward using Euclid's algorithm. For Exercise 2, we use the fact that $\gcd(168, 252, 294) = \gcd(\gcd(168, 252), 294)$.

Exercise 3. *Find integers x and y such that $13x + 15y = 1$.*

Proof. Let $x = 7$ and $y = -6$. Then $13x + 15y = 1$. □

In the above exercise, the Bézout's coefficients x and y can be found using Euclidean algorithm.

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

Proof. Consider the canonical decompositions (prime factorizations): $2 \cdot 3 \cdot 5$, $3 \cdot 5 \cdot 7 \cdot$, $5 \cdot 7 \cdot 11$ 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.*

Proof. 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 $(d, b) = 1$.*

Proof. 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 $(u, v) = (u', v')$.*

Proof.

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* $(a_0, a_1, a_2) \sim (25/6, -5, 10/3)$.

Proof. 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).

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 $x, y \in H$.*

Proof. Suppose H is a subgroup of G. That is, H is a group in its own right, and all the group axioms hold in H. Let $x, y \in H$. Then, $-y \in H$ (existence of inverse) and $x - y = x + (-y) \in H$ (closure). Conversely, suppose $x - y \in H$ for all $x, y \in H$. Clearly $0 \in H$ since $x - x = 0$ for any $x \in H$. Also, $-x \in H$ for any $x \in H$ since $-x = 0 - x$. Finally for any $x, y \in H$, we see that $x + y = x - (-y) \in H$. It follows that H is a subgroup. □

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 $\mathbb{Z}$.*

Proof. 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 $\mathbb{Z}$.

Proof. 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.*

PROOF. 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.*

PROOF. Let $x, y \in \ker(f)$. Then $f(x+y) = f(x) + f(y) = e + e = e$ and so, $x + y \in \ker(f)$. We must be careful that the two operations $+$ mean different things: the first one is between elements in G; the second one is between elements in H. Let e_G be the identity element of G. Clearly $f(x) = f(x + e_G) = f(x) + f(e_G)$ for every $x \in G$, and so, $f(e_G) = e$. That is, $e_G \in \ker(f)$. Finally, $e = f(e_G) = f(x - x) = f(x) + f(-x) = e + f(-x) = f(-x)$ for every $x \in \ker(f)$. That is, $-x \in \ker(f)$ for every $x \in \ker(f)$. It follows that $\ker(f)$ is a subgroup of G. Let I be the image of f in H. Since $f(e_G) = e$, we see that $e \in I$. Let $x, y \in I$. Then there exists $a, b \in G$ such that $f(a) = x$ and $f(b) = y$. Clearly $f(a + b) = f(a) + f(b) = x + y$ so that $x + y \in I$. Also, $e = f(e_G) = f(a - a) = f(a) + f(-a) = x + f(-a)$ so that $-x = f(-a)$. That is, $-x \in I$ for all $x \in I$. Consequently, I is a subgroup of H. □

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.*

PROOF. 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 $f(k) = e^{2\pi ik/m}$ is a group homomorphism. What is the kernel of this homomorphism?*

PROOF. Let $h, k \in \mathbb{Z}$. Then $f(h + k) = e^{2\pi i(h+k)/m} = e^{2\pi ih/m} \cdot e^{2\pi ik/m} = f(h) \cdot f(k)$. This proves the homomorphism. Let $k \in \ker(f)$. Then $f(k) = e^{2\pi ik/m} = 1$, 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 $0 \leq x < 1$. We define* *a binary operation $x * y$ for numbers $x, y \in G$ as follows:*

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

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.

Proof. 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 $\{x\} = 1/\langle a_1, a_2, \ldots, a_N \rangle$.*

Proof. 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. *Let $\frac{a}{b}$ be a rational number that is not an integer. Prove that there exist unique integers $a_0, a_1, \ldots, a_N$ such that $a_i \geq 1$ for $i = 1, \ldots, N-1, a_N \geq 2$, and*

$$\frac{a}{b} = \langle a_0, a_1, \ldots, a_{N-1}, a_N \rangle.$$

Proof. Let $a/b = \langle a_0, a_1, \ldots, a_{N-1}, a_N \rangle = \langle b_0, b_1, \ldots, b_{N-1}, b_N \rangle$. Then, by Exercise 7, $a_0 = [a/b] = b_0$, and

$$\langle a_1, \ldots, a_N \rangle = \frac{1}{\{a/b\}} = x_1 \text{ (say)}.$$

By Exercise 7 again, $a_1 = [x_1] = b_1$, and

$$\langle a_2, \ldots, a_N \rangle = \frac{1}{\{x_1\}} = x_2 \text{ (say)}.$$

Since $0 < \{a/b\} < 1$, we must have $x_1 = 1/\{a/b\} > 1$. Thus, $a_1 \geq 1$. Continuing this further, we obtain $a_i = b_i$ for all $0 \leq i \leq N$ such that $a_i \geq 1$ for $i = 1, \ldots, N-1$, $a_N \geq 2$. The last step (Nth) should be careful for we can write 2 as $1 + \frac{1}{1}$. Therefore, we make it sure that $a_N \geq 2$ to remove this ambiguity. □

Exercise 9. *Prove that*

$$\langle a_0, a_1, \ldots, a_N, a_{N+1} \rangle = \langle a_0, a_1, \ldots, a_N + \frac{1}{a_{N+1}} \rangle.$$

Proof. This should be obvious since both of them have the same expansion given below

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots \cfrac{1}{\ldots + \cfrac{1}{a_N + \cfrac{1}{a_{N+1}}}}}}.$$

Therefore, $\langle a_0, a_1, \ldots, a_N, a_{N+1} \rangle = \langle a_0, a_1, \ldots, a_N + \frac{1}{a_{N+1}} \rangle$. □

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 $\langle a_0, a_1, \ldots, a_N \rangle$.

Proof. We prove this using induction on n. The base case of $n = 0$ follows immediately. 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 $n = k$. That is,

$$\langle a_0, a_1, \ldots, a_k \rangle = \frac{p_k}{q_k} = \frac{a_k p_{k-1} + q_{k-2}}{a_k q_{k-1} + q_{k-2}}.$$

Since $\langle a_0, a_1, \ldots, a_k, a_{k+1} \rangle = \langle a_0, a_1, \ldots, a_k + 1/a_{k+1} \rangle$, it follows that

$$\begin{aligned}
\langle a_0, a_1, \ldots, a_k, a_{k+1} \rangle &= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} \\
&= \frac{(a_k a_{k+1} + 1) p_{k-1} + a_{k+1} p_{k-2}}{(a_k a_{k+1} + 1) q_{k-1} + a_{k+2} q_{k-2}} \\
&= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} \\
&= \frac{p_{k+1}}{q_{k+1}},
\end{aligned}$$

By induction, the proposition follows. □

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 $n = 0, 1, \ldots, N$.

Proof. We may write

$$\begin{aligned} p_n q_{n-1} - p_{n-1} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2}) \\ &= -(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \\ &= (-1)^2 (p_{n-2} q_{n-3} - p_{n-3} q_{n-2}) \\ &= \cdots \\ &= \cdots \\ &= (-1)^{n-1} (p_1 q_0 - q_0 p_1) \\ &= (-1)^{n-1}. \end{aligned}$$

If $a_i \in \mathbb{Z}$ for $i = 0, 1, \ldots, N$, then $p_n, q_n \in \mathbb{Z}$ for each $0 \leq n \leq N$. Suppose $\gcd(p_n, q_n) = d > 1$. We have proved that $p_n q_{n-1} - p_{n-1} q_n = (-1)^n$. Then d would divide ± 1, which is absurd. It follows that $\gcd(p_n, q_n) = 1$. □

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 $n = 2, \ldots, N$.

Proof. By Exercise 12, we have

$$\begin{aligned} p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2}(a_n q_{n-1} + q_{n-2}) \\ &= a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \\ &= (-1)^n a_n . \square \end{aligned}$$

Exercise 14. *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,*

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

Proof. By Exercise 13, we have

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

Since a_n, q_n, q_{n-2} are positive integers, this difference has the same sign as $(-1)^n$. Therefore, the even convergents are strictly increasing while the odd convergents are strictly decreasing. Thus, we have now proved

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

We shall now prove that every odd convergent is greater than any even convergent. By Exercise 12, we see that

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

and so, this difference has the same sign as $(-1)^{n-1}$. Looking at the case when n is odd, it is easy to see that every odd convergent is greater than its predecessor and its successor. Combined with an earlier result we have proved, it follows that every odd convergent is greater than any even convergent. A particular case also shows

$$\frac{p_0}{q_0} < x < \frac{p_1}{q_1}.$$

Therefore, we have proved that

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

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

$$\begin{aligned} &f_0 = 0, \\ &f_1 = 1, \\ &f_n = f_{n-1} + f_{n-2} \textit{ for } n \geq 2. \end{aligned}$$

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.

Proof. 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.

Proof. 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.

Proof. Using the Fibonacci recurrence relation, we obtain

$$\begin{aligned} f_{n+1}f_{n-1} - f_n^2 &= (f_n + f_{n-1})f_{n-1} - f_n^2 \\ &= f_n f_{n-1} + f_{n-1}^2 - f_n^2 \\ &= f_n(f_{n-1} - f_n) + f_{n-1}^2 \\ &= (-1)(f_n f_{n-2} - f_{n-1}^2) \\ &= (-1)^2(f_{n-1}f_{n-3} - f_{n-2}^2) \\ &= \cdots \\ &= \cdots \\ &= (-1)^{n-1}(f_2 f_0 - f_1^2) \\ &= (-1)^n, \end{aligned}$$

where we have used $f_2 f_0 - f_1^2 = -1$. □

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, $f_n = f_{n-1} + f_{n-2} = 2f_{n-2} + f_{n-3} = 3f_{n-3} + 2f_{n-4} = 5f_{n-4} + 3f_{n-5} \cdots$.

Proof. 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.*

Proof. We prove this proposition by induction on l. The base case of $l = 1$ follows trivially. Suppose the proposition holds for $l = k$ for some $k \in \mathbb{Z}, k > 1$. By the result of Exercise 19, we can write

$$f_{(k+1)n} = f_{kn+n} = f_{n+1}f_{kn} + f_n f_{kn-1}.$$

Since f_n divides f_{kn} (by induction hypothesis) and f_n, it follows that f_n divides $f_{(k+1)n}$. The proposition follows. □

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

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

PROOF. 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!.

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

$$\begin{aligned} v_2(15!) &= \left[\frac{15}{2}\right] + \left[\frac{15}{4}\right] + \left[\frac{15}{8}\right] = 7 + 3 + 1 = 11, \\ v_3(15!) &= \left[\frac{15}{3}\right] + \left[\frac{15}{9}\right] = 5 + 1 = 6, \\ v_5(15!) &= \left[\frac{15}{5}\right] = 3, \\ v_7(15!) &= \left[\frac{15}{7}\right] = 1, \\ v_{11}(15!) &= \left[\frac{15}{11}\right] = 1, \\ v_{13}(15!) &= \left[\frac{15}{13}\right] = 1. \end{aligned}$$

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 $n = 3$.*

PROOF. 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 $n = 3$.*

PROOF. 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.*

PROOF. 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.*

PROOF. 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.*

PROOF. 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.*

PROOF. Suppose p and q are twin primes. Without loss of generality, we assume $q = p+2$. Then $pq+1 = p(p+2)+1 = p^2+2p+1 = (p+1)^2$, which is a square. Conversely, suppose p and q are two primes with $pq+1 = a^2$ for some $a \in \mathbb{Z}$. Then $pq = a^2 - 1 = (a+1)(a-1)$. But p and q are primes, and the only factors they have are 1 and themselves. It follows that $a+1$ and $a-1$ are p and q themselves so that $|p-q| = |(a+1)-(a-1)| = 2$. Therefore, p and q are twin primes. The proposition follows. □

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

PROOF. 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*

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

PROOF. 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.*

PROOF. Suppose d divides m. That is, there exists an integer c such that $m = dc$. Suppose d has p as one of its prime divisors. Clearly $v_p(d) \leq v_p(m)$ (otherwise the relation $m = dc$ will not hold). If p is not a prime divisor of d, then the relation trivially holds since $v_p(d) = 0$. Conversely, suppose $v_p(d) \leq v_p(m)$ for all primes p. Then

$$\frac{m}{d} = \frac{\prod_{i=1} p_i^{v_{p_i}(m)}}{\prod_{i=1} p_i^{v_{p_i}(d)}} = \prod_{i=1} p_i^{v_{p_i}(m)-v_{p_i}(d)}$$

is an integer. Consequently, d divides m. □

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 $m_i = mp_i^{-r_i}$ for $i = 1, \ldots, k$. Prove that $(m_1, \ldots, m_k) = 1$.*

PROOF. Let $M = \{m_1, \ldots, m_k\}$ and $P = \{p_1, \ldots, p_k\}$. To prove that $\gcd(m_1, \ldots, m_k) = 1$, it suffices to prove that there is no prime in P that divides all $m_i \in M$. Suppose there is a prime $p_j \in P$ that divides $m_i \in M$ for all $1 \leq i \leq k$. Then p_j also divides m_j. But $m_j = p_j^{-r_j} m = p_j^{-r_j} \prod_{i=1}^{k} p_i^{r_i}$, that is, m_j does not have p_j in its prime factorization, which is absurd. It follows that $\gcd(m_1, \ldots, m_k) = 1$ □

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

PROOF. Suppose $(ab, c) = 1$. That is, there is no prime that divides ab and c, which is essentially the same as saying there is no prime that divides a and c, and there is no prime that divides b and c. Consequently, $\gcd(a, c) = \gcd(b, c) = 1$. The other direction can be argued similarly. □

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.*

PROOF. 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.*

PROOF. We shall provide a constructive proof. Let $d = \prod_{i=1}^{k} p_i^{r_i}$ be its prime factorization. Since d divides m, it follows that $m = z \prod_{i=1}^{k} p_i^{r_i}$ for some integer $z \in \mathbb{Z}$. Since d is composite, there are at least two primes that divide d (the two primes may not be distinct). Let p_j be some prime factor of d. We construct b and c as follows:

$$b = z\frac{\prod_{i=1}^{k} p_i^{r_i}}{p_j^{r_j}}, \qquad c = p_j^{r_j},$$

so that $m = bc$. If z has no p_j in its prime factorization, and $k > 1$, then we are done (because, d does not divide b nor c). Suppose z has p_j in its prime factorization. Then we move $p_j^{v_{p_j}(z)}$ from z in b to c (in other words, we are making sure that d does not divide b). If $k = 1$, a similar construction works (assuming each prime is distinct). In all the cases, d does not divide b nor c but $m = bc$. The proposition follows. □

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 $(a, b) = 1$.*

Proof. Suppose $\gcd(a, b) = 1$. There is no prime that divides both a and b. Whatever common prime factor a and bc has, it must be a common prime factor of a and c. It follows that $\gcd(a, bc) = \gcd(a, c) = \gcd(a, b)\gcd(a, c)$.

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 $d = d_1 \cdots d_k$.*

Proof. 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

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

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. □

Exercise 22. *Let $n \geq 2$, and let x be a rational number. Prove that $\sqrt[n]{x}$ is rational if and only if $x = y^n$ for some rational number y.*

Proof. Suppose $x = y^n$ for some rational number y. Then $\sqrt[n]{x} = \sqrt[n]{y^n} = y$, which is rational. Conversely, suppose $\sqrt[n]{x}$ is rational. Then $\sqrt[n]{x} = \frac{p}{q}$ for some integers $p, q \neq 0$ so that $x = (\frac{p}{q})^n = y^n$, where $y = p/q$ is a rational number. □

Exercise 23. *Let $m_1, \ldots, m_k$ be positive integers and $m = [m_1, \ldots, m_k]$. Prove that there exist positive integers $d_1, \ldots, d_k$ such that d_i is a divisor of m_i for $i = 1, \ldots, k, (d_i, d_j) = 1$ for $1 \leq i < j \leq n$, and $m = [d_1, \ldots, d_k] = d_1 \cdots d_k$.*

Proof. Let $m = [m_1, \ldots, m_k] = \prod_{i=0}^{N} p_i^{r_i}$ be its prime factorization. We pick p_1 (the first prime that divides m). Clearly there is at least one number m_i such that its prime factorization has $p_1^{r_1}$ as its factor. If there are multiple such m_i's we choose the one that comes first, that is, the one with the smallest index i. Suppose m_j is the number chosen under this convention.

Then we put $p_1^{r_1}$ into a new set M_j. Likewise, we pick p_2, and repeat the same process. In fact, we go through this process for all primes that divide m. After that is done, if M_i does not already exist for any $1 \leq i \leq k$, we construct M_i and let $M_i = \{1\}$. Then we construct the following k numbers:

$$d_i = \begin{cases} \prod p_i^{r_i} & \text{where } p_i^{r_i} \in M_i, \\ 1 & \text{if } M_i = \{1\}. \end{cases}$$

We observe that d_i divides m_i for all $1 \leq i \leq k$. Also, $\gcd(d_i, d_j) = 1$ for all $1 \leq i, j \leq k$ (because, by our construction, no prime p_i will divide both d_i and d_j). Consequently $m = [d_1, \ldots, d_k] = d_1 \cdots d_k$. □

EXERCISE 24. *Prove that for any positive integers a and b,*

$$[a, b] = \frac{ab}{(a, b)}.$$

PROOF. Let $a = \prod p^{v_p(a)}$ and $b = \prod p^{v_p(b)}$ be their prime factorizations so that

$$(a, b) = \prod p^{\min\{v_p(a), v_p(b)\}}, \qquad [a, b] = \prod p^{\max\{v_p(a), v_p(b)\}}.$$

Since $\min\{v_p(a), v_p(b)\} + \max\{v_p(a), v_p(b)\} = v_p(a) + v_p(b)$, it follows that

$$(a, b)[a, b] = \prod p^{\min\{v_p(a), v_p(b)\} + \max\{v_p(a), v_p(b)\}} = \prod p^{v_p(a) + v_p(b)} = ab.$$

The proposition follows. □

EXERCISE 25. *Let a and b be positive integers with $(a, b) = d$. Prove that*

$$\left[\frac{a}{d}, \frac{b}{d}\right] = \frac{[a, b]}{d}.$$

PROOF. Let $a = \prod p^{v_p(a)}$ and $b = \prod p^{v_p(b)}$ be their prime factorizations so that

$$d = \gcd(a, b) = \prod p^{\min\{v_p(a), v_p(b)\}},$$

and

$$\frac{a}{d} = \prod p^{v_p(a) - \min\{v_p(a), v_p(b)\}}, \qquad \frac{b}{d} = \prod p^{v_{p(b)} - \min\{v_p(a), v_p(b)\}}.$$

We see that $\max\{v_p(a) - \min\{v_p(a), v_p(b)\}, v_{p(b)} - \min\{v_p(a), v_p(b)\}\} = \max\{v_p(a), v_p(b)\} - \min\{v_p(a), v_p(b)\}$. Therefore,

$$\begin{aligned} \left[\frac{a}{d}, \frac{b}{d}\right] &= \prod p^{\max\{v_p(a) - \min\{v_p(a), v_p(b)\}, v_{p(b)} - \min\{v_p(a), v_p(b)\}\}} \\ &= \prod p^{\max\{v_p(a), v_p(b)\} - \min\{v_p(a), v_p(b)\}} \\ &= \prod p^{\max\{v_p(a), v_p(b)\}} / \prod p^{\min\{v_p(a), v_p(b)\}} \\ &= \frac{[a, b]}{d}. \end{aligned}$$

The proposition follows. □

Exercise 26. *Prove that for any positive integers a, b, c,*

$$[a, b, c] = \frac{abc(a, b, c)}{(a, b)(b, c)(c, a)}.$$

Proof. Considering how we tackled Exercises 24-25, it suffices to prove that

$$\max\{v_p(a), v_p(b), v_p(c)\} = \frac{v_p(a)v_p(b)v_p(c) \min\{v_p(a), v_p(b), v_p(c)\}}{\min\{v_a(p)v_b(p)v_c(p)\}},$$

or rather

$$\max\{x, y, z\} = \frac{xyz \min\{x, y, z\}}{\min\{x, y\} \min\{y, z\} \min\{z, x\}},$$

where x, y, z are any three positive integers. Clearly maximum and minimum functions are symmetric, that is, the order in which its arguments are written makes no difference. For instance, $\max\{x, y, z\} = \max\{y, z, x\}$. Thus, without loss of generality, we may assume $x \leq y \leq z$. Using this relation, we verify the equation we have written above. Indeed, both the left hand side and right hand side evaluate to z, and we are done. □

Exercise 27. *Let $a_1, \ldots, a_k$ be positive integers. Prove that $[a_1, \ldots, a_k] = a_1 \cdots a_k$ if and only if the integers $a_1, \ldots, a_k$ are pairwise relatively prime.*

Proof. Suppose $[a_1, \ldots, a_k] = a_1 \cdots a_k$. It follows that

$$\max\{v_p(a_1), \ldots, v_p(v_k)\} = \sum_{i=1}^{k} v_p(a_i)$$

for each prime p appearing in the factorization of $[a_1, \ldots, a_k]$, which is possible only when $v_p(a_i) = 0$ for all i with one exception. So, any prime p dividing m_j will not divide any other m_i with $i \neq j$. It follows that the integers $a_1, \ldots, a_k$ are pairwise relatively prime. Conversely, suppose $\gcd(a_i, a_j) = 1$ for all $1 \leq i, j \leq k$. It is easy to see that the above equation holds, and so the proposition is true. □

Exercise 28. *Let a and b be positive integers and p a prime. Prove that if p divides $[a, b]$ and p divides $a + b$, then p divides (a, b).*

Proof.

Exercise 31. *A positive integer is called square-free if it is the product of distinct prime numbers. Prove that every positive integer can be written uniquely as the product of a square and a square-free integer.*

Proof. Let a be any positive integer and let $a = \prod_{i=1}^{k} p_i^{r_i}$ be its prime factorization. We pick the first prime p_1. If r_1 is odd, we can write $p \cdot p^{r_i - 1}$ so that $r_i - 1$ is even and so, $p^{r_i - 1}$ is a square. If r_1 is even, we leave it as it is (because it is already a square). We repeat the process for each prime p_i where $1 \leq i \leq k$. Thus, we are left with distinct primes p_i and squares $p_i^{r_i}$ (or $p_i^{r_i - 1}$). The product of these distinct primes is a radical and the product of the squares is a square. Therefore, a is written as the product of a square and a square-free integer. The uniqueness follows from the fact that this is the only way to write a as the product of a square and a square-free integer (this is implicit in the construction we have used). □

EXERCISE 32. *Prove that the set of all rational numbers of the form a/b, where $a, b \in \mathbb{Z}$ and b is square-free, is an additive subgroup of $\mathbb{Q}$.*

PROOF. Let S be the set of all rational numbers of the form a/b, where $a, b \in \mathbb{Z}$ and b is square-free. Clearly $0 \in S$. It is easy to see that 0 is the identity element in S (after all, S is a subset of $\mathbb{Q}$). If $x \in S$, then $-x \in S$ (after all, they have the same denominator) such that $x + (-x) = 0 = (-x) + x$. Let $x, y \in S$. It is easy to see that $x + y \in S$. This is because the denominator of $x + y$ is the lowest common multiple (lcm) of the denominators of x and y, but the highest power of any prime in the denominators of x and y is the prime itself so that the lcm contains only distinct primes. It follows that S is an additive subgroup of $\mathbb{Q}$. □

EXERCISE 33. A powerful number is a positive integer n such that if a prime p divides n, then p^2 divides n. Prove that every powerful number can be written as the product of a square and a cube. Construct examples to show that this representation of powerful numbers is not unique.

PROOF. Let n be a powerful number. Since p^2 divides n whenever p divides n, it follows that n has a prime factorization of the form $n = \prod_{i=1}^{k} p_i^{r_i}$ such that $r_i \geq 2$ for all $1 \leq i \leq k$. We pick the first prime p_1. Either r_1 is odd or even. If r_1 is odd, then we can write $r_1 = 3 + r_1'$ (and hence $p^{r_1} = p^3 \cdot p^{r_1'}$) where r_1' is even. This is possible because $r_i \geq 2$. We continue this for all primes p_i appearing in the factorization of n. The product (say b) of all even powers of primes is a square and the product (say c) of all cubes of primes is definitely a cube, so that $n = bc$. It is easy to see that, unlike Exercise 34, this construction is not unique. For instance, we could write p^6 as either $(p^2 p^2)^2$ (which is a square) or $(p^2)^3$ (which is a cube). □

EXERCISE 34. *Prove that m is square-free if and only if* $\operatorname{rad}(m) = m$.

PROOF. Suppose m is square-free. Then m is a product of distinct primes. If follows that $\operatorname{rad}(m) = m$. Conversely, suppose $\operatorname{rad}(m) = m$. This is possible only when the highest power of every prime that divides m is the prime itself. Consequently, m is a product of distinct primes, and so m is square-free. □

EXERCISE 35. *Prove that* $\operatorname{rad}(mn) = \operatorname{rad}(m) \operatorname{rad}(n)$ *if and only if* $(m, n) = 1$.

PROOF. Suppose $\operatorname{rad}(mn) = \operatorname{rad}(m) \operatorname{rad}(n)$. Since the left hand side is a product of distinct primes, it follows that $\operatorname{rad}(m)$ and $\operatorname{rad}(n)$ have no prime factor in common. But every prime factor of m is also a factor of $\operatorname{rad}(m)$. Likewise for n. Therefore, m and n have no prime factor in common. Consequently, $\gcd(m, n) = 1$. The argument for the other direction is similar. □

EXERCISE 36. *Let $H = \{1, 5, 9, \dots, \}$ be the arithmetic progression of all positive integers of the form $4k + 1$. Elements of H are called Hilbert numbers. Show that H is closed under multiplication, that is, $x, y \in H$ implies $xy \in H$. An element x of H will be called a Hilbert prime if $x \neq 1$ and x cannot be written as the product of two strictly smaller elements of H. Compute all the Hilbert primes up to* 100. *Prove that every element of H can be factored into a product of Hilbert primes, but that unique factorization does not hold in H.*

Proof. Let $a = 4k+1$ and $b = 4h+1$ be any two elements of H. Then $ab = (4k+1)(4h+1) = 4(4kh + k + h) + 1$ is in H and so, H is closed under multiplication. By computation, all the Hilbert primes less than 100 are 5, 9, 13, 17, 21, 29, 33, 37, 41, 49, 53, 57, 61, 69, 73, 77, 81, 89, 93, and 97. In computing these numbers, we use prime factorization to see if the number can be factored into Hilbert numbers. From the definition of Hilbert prime given in the question, proving that every element of H can be factored into a product of Hilbert primes is rather very simple. If a Hilbert number (say a) can be factored into a product of Hilbert primes, then we are done. Otherwise, a is a Hilbert prime and hence we have obtained its factorization. This factorization is not unique. For example, $441 = 9 \cdot 49 = 21 \cdot 21$. □

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.*

Proof. Suppose $a^n - 1$ is prime. But $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$. So, $a - 1 = 1$, that is, $a = 2$. Suppose n is composite. Let $n = hk$ for some $1 < h, k < n$. Then $a^{hk} - 1 = (a^h - 1)[(a^h)^{k-1} + (a^h)^{k-2} + \cdots + a^h + 1]$, that is, $a^h - 1$ is composite which is absurd. Therefore, $n = p$ is prime. The first five Mersenne primes are 3, 7, 31, 127, and 8191. □

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 $n = 1, 2, 3, 4$.

Proof. We shall prove the proposition by proving its contrapositive. Suppose $k \neq 2^n$. Then k has an odd prime $h > 1$ as its factor. So, $k = lh$ for some $1 \leq l < k$. A consequence of binomial theorem states that $a - b$ divides $a^m - b^m$ for any $a, b, m \in \mathbb{Z}, m > 0$. Putting $a = 2^l, b = -1$, and $m = h$, we see that $2^l + 1$ divides $2^{lh} + 1$, that is, $2^k + 1$ is composite. Therefore, k must be a power of 2. By computation, we obtain $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$. The first three Fermat numbers are obviously prime. To check that 65537 is prime, we check that no prime less than 256 (because $\sqrt{65537} \sim 256$) divides 65537. □

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

Proof. 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.

PROOF. 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* $n \geq 8$.

PROOF.

1.6 A Linear Diophantine Equation

EXERCISE 1. *Prove that the equation*

$$3x_1 + 5x_2 = b$$

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

PROOF. Since $\gcd(3,5) = 1$, the equation has a Proof 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 Proofs in nonnegative integers* x_1 *and* x_2 *of the linear diophantine Proof*

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

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

$$\begin{aligned} 2 \cdot 23 + 7 \cdot 1 &= 53, \qquad & 2 \cdot 9 + 7 \cdot 5 &= 53, \\ 2 \cdot 16 + 7 \cdot 3 &= 53, \qquad & 2 \cdot 2 + 7 \cdot 7 &= 53. \end{aligned}$$

□

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*

$$a_1x_1 + a_2x_2$$

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

PROOF. 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.

$$\begin{aligned} &V(0,0) = 0, \quad &&V(1,0) = 3, \quad &&V(2,0) = 6, \\ &V(3,0) = 9, \quad &&V(4,0) = 12, \quad &&V(5,0) = 15, \\ &V(0,1) = 10, \quad &&V(1,1) = 13, \quad &&V(2,1) = 16. \end{aligned}$$

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 $N(3,10)/G(3,10) = 1/2$. □

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 $G(3,10,14)$.

Proof. 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 $G(3,10,14) = 12$. □

Exercise 8 is similar to Exercise 2.

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

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

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

$$\begin{aligned} 3x_1 + 5x_2 &= 560 - 7k, \\ 9x_1 + 25x_2 &= 2920 - 49k, \end{aligned}$$

whose Proofs, 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 Proofs, 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 Proof is $(15, 82, 15)$. □

Exercise 10. *Find all Proofs of the Ramanujan-Nagell diophantine equation*

$$x^2 + 7 = 2^n$$

with $x \leq 1000$.

Proof. We observe that $1000^2 = 1000000$, and $2^{20} = 1048576$. Thus, we need only check for $n < 20$. Since powers of 2 are even, $x^2 + 7$ must be even, that is, x^2 must be odd. It follows that x must be odd. Clearly it has no Proofs when $n < 3$. We look at the values $\sqrt{2^n - 7}$ for each $3 \leq n \leq 19$ and see if it evaluates to an odd integer. We shall write a Proof in the form (x, n). An obvious Proof is $(1, 3)$. Other Proofs are $(3, 4)$, $(5, 5)$, $(11, 7)$, and $(181, 15)$. It is checked that these are all the possible Proofs. □

Exercise 11. *Find all Proofs of the Ljunggren diophantine equation*

$$x^2 - 2y^4 = -1$$

with $x \leq 1000$.

Proof. We can re-write the equation as $x^2 + 1 = 2y^4$. We observe that $1000^2 = 1000000$ and $27^4 = 531441$. Thus, we need only check for $n < 27$. As in Exercise 10, we shall write a Proof in the form (x, y). An obvious Proof is $(1, 1)$. It is checked that the only other Proof is $(239, 13)$. □

2 Congruences

2.1 The Ring of Congruence Classes

Exercise 1. *Compute the least nonnegative residue of* $10^k + 1$ *modulo* 13 *for* $k = 1, 2, 3, 4$.

Proof. We compute

$$\begin{aligned} 10^1 + 1 &\equiv 10 \mod 13, & 10^3 + 1 &\equiv 12 \mod 13, \\ 10^2 + 1 &\equiv 9 \mod 13, & 10^4 + 1 &\equiv 3 \mod 13. \end{aligned}$$

We simply computed the remainders on division by 13. □

Exercise 2. *Compute the least nonnegative residue of* 5^{22} *modulo* 23.

Proof. We observe that 23 is a prime. Therefore, Fermat's theorem, $5^{22} \equiv 1 \mod 23$. □

Exercise 3. *Construct the multiplication table for the ring* $\mathbb{Z}/5\mathbb{Z}$.

Proof. We see that $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$. To construct the multiplication table, we compute all the products $a \cdot b$ for $a, b \in \mathbb{Z}/5\mathbb{Z}$.

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

□

Exercise 4. *Construct the multiplication table for the ring* $\mathbb{Z}/6\mathbb{Z}$.

Proof. We see that $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$. As in Exercise 3, we compute all products $a \cdot b$ for $a, b \in \mathbb{Z}/6\mathbb{Z}$. □

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, $\ldots$, $2m - 2$.

Proof. 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 $-q \leq r \leq q$.*

Proof. As in Exercise 6, we only need to find the correct map. Let $X = \{0, 1, 2, \dots, 2q\}$ be the complete set of residues modulo $2q+1$. Let $Y = \{-q, -q+1, \dots, q-1, q\}$. 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 $-(q-1) \leq r \leq q$.*

Proof. Let $X = \{0, 1, 2, \dots, 2q-1\}$ be the complete set of residues modulo $2q$. Let $Y = \{-(q-1), -q+2, \dots, q-1, q\}$. 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.*

Proof. 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.*

Proof. 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) $a^4 - 1 = 5^4a^4 + 4 \cdot 5^3a^3 \cdot 2 + 6 \cdot 5^2a^2 \cdot 2^2 + 4 \cdot 5a \cdot 2^3 + 15$, 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.

Exercise 13. *Let d be a positive integer that is a common divisor of a, b, and m. Prove that*

$$a \equiv b \mod m$$

if and only if

$$\frac{a}{d} \equiv \frac{b}{d} \mod \frac{m}{d}.$$

Proof. Suppose $a \equiv b \mod m$. That is, m divides $a-b$. Or rather, $(a-b)/m$ is an integer. Then $\frac{(a-b)/d}{m/d}$ is also an integer. That is, m/d divides $(a-b)/d$. Or rather,

$$\frac{a}{d} \equiv \frac{b}{d} \mod \frac{m}{d}.$$

The converse can be checked similarly. □

EXERCISE 15. *Prove that $a_1 \equiv a_2 \mod m$ implies $a_1^k \equiv a_2^k \mod m$ for all $k \geq 1$. Prove that if $f(x)$ is a polynomial with integer coefficients and $a_1 \equiv a_2 \mod m$, then $f(a_1) \equiv f(a_2) \mod m$.*

PROOF. Suppose $a_1 \equiv a_2 \mod m$. That is, m divides $a_1 - a_2$. But then $a_1^k - a_2^k = (a_1 - a_2)(a_1^{k-1} + a_1^{k-2}a_2 + \cdots + a_1a_2^{k-2} + a_2^{k-1})$, and so $a_1 - a_2$ divides $a_1^k - a_2^k$. It follows that m divides $a_1^k - a_2^k$. Therefore, $a_1^k \equiv a_2^k \mod m$ for all $k \geq 1$. We observe that $a_1 \equiv a_2 \mod m$ also implies $ca_1 \equiv ca_2 \mod m$ for any integer c. Also, $a_1 \equiv a_2 \mod m$ and $a_3 \equiv a_4 \mod m$ implies $a_1 + a_3 \equiv a_2 + a_4 \mod m$. Indeed, when we think of it in terms of divisibility by m, it becomes trivial. Let $f(x) = c_nx^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ where $c_i \in \mathbb{Z}$ for $0 \leq i \leq n$. Since $a_2 \equiv a_2 \mod m$, by the implications we have derived above, $f(a_1) \equiv f(a_2) \mod m$. □

EXERCISE 16. *(A criterion for divisibility by 9). Prove that a positive integer n is divisible by 9 if and only if the sum of its decimal digits is divisible by 9. (For example, the sum of the decimal digits of 567 is $5 + 6 + 7 = 18$.)*

PROOF. Since $a^m - b^m = (a - b)(a^{m-1} + a^{m-2}b + \cdots + ab^{m-2} + b^{m-1})$ for a positive integer m so that $a - b$ divides $a^m - b^m$. Substituting $a = 10$, and $b = 1$, it follows that 9 divides $10^m - 1$. In other words, $10^m \equiv 1 \mod 9$. Let x be any decimal number (base 10). Suppose $x = a_ka_{k-1} \cdots a_1a_0$ where $a_0, a_1, \ldots, a_k$ are its decimal digits. Then it has a unique 10-acidic representation of the following form

$$x = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k.$$

This is simply the representation which are used to. Since $10^i \equiv 1 \mod 9$, it follows that $a_i \cdot 10^i \equiv a_i \mod 9$. Summing this congruence over $0 \leq i \leq k$, we obtain

$$x \equiv \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \mod 9.$$

Therefore, $x \equiv 0 \mod 9$ if and only if $\sum_{i=0}^{k} a_i \equiv 0 \mod 9$. In other words, a decimal number is divisible by 9 if and only if the sum of its digits is divisible by 9. □

EXERCISE 17. *(A criterion for divisibility by 11.) Prove that a positive integer n is divisible by 11 if and only if the alternating sum of its decimal digits is divisible by 11. (For example, the alternating sum of the decimal digits of 80,729 is $-9 + 2 - 7 + 0 - 8 = -22$.)*

PROOF.

EXERCISE 18. *Prove that if $x_1, \ldots, x_m$ is a sequence of m not necessarily distinct integers, then there is a subsequence of consecutive terms whose sum is divisible by m, that is, there exists integers $1 \leq k \leq l \leq m$ such that*

$$\sum_{i=k}^{l} x_i \equiv 0 \mod m.$$

PROOF. We consider the $m+1$ integers $0, x_1, x_1+x_2, x_1+x_2+x_3, \ldots, x_1+x_2+\cdots+x_m$. We shall represent them as s_i where $0 \leq i \leq m$ (because s reminds us of sum!). There are $m+1$

such sums (s_i) while there are only m numbers in the complete set of residues modulo m. By pigeonhole principle, there are two sums s_i and s_j (say) such that $s_i \equiv s_j \mod m$. Without loss of generality, we assume that $i < j$. Then $s_j - s_i \equiv 0 \mod m$. That is,

$$x_{i+1} + x_{i+2} + \cdots + s_j \equiv 0 \mod m.$$

The proposition follows. □

Exercise 19. *Let $m \geq 2$ and let d be a positive divisor of $m-1$. Let $n = a_0 + a_1 m + \cdots + a_k m^k$ be the m-acidic representation of n. Prove that $n \equiv 0 \mod d$ if and only if $a_0 + a_1 + \cdots + a_k \equiv 0 \mod d$.*

Proof. Since d divides $m-1$, we conclude that d also divides $m^k - 1$ for any nonnegative integer k (because $m-1$ divides m^k-1, see Exercise 16), and so $m^k \equiv 1 \mod d$. By a result of Exercise 15,

$$n \equiv \sum_{i=0}^{k} a_i m^i \equiv \sum_{i=0}^{k} a_i \mod d,$$

so that $n \equiv 0 \mod d$ if and only if $a_0 + a_1 + \cdots + a_k \equiv 0 \mod d$. □

Exercise 20. *Prove that every integer belongs to at least one of the following 6 congruence classes:*

$$\begin{array}{rl} 0 & \mod 2 \\ 0 & \mod 3 \\ 1 & \mod 4 \\ 3 & \mod 8 \\ 7 & \mod 12 \\ 23 & \mod 24. \end{array}$$

Proof. Let n be any integer. Then n is of the form $24k + a$ where $0 \leq a \leq 23$. Indeed, a is simply the remainder on division of n by 24. We shall prove that any $24k + a$ with $0 \leq a \leq 23$ can be reduced to one of the forms (or congruence classes) given in the question. All even numbers, that is, numbers of the form $24k + a$ where a is even is equivalent to $2k$ or they belong to the congruence class ($0 \mod 2$). Similarly, numbers of the form $24k + a$ where a is a multiple of 3 is equivalent to $3k$ or they belong to the congruence class ($0 \mod 3$). We are left with only the forms $24k + a$ where a is neither even nor multiple of 3. The form $24k + 1$ is equivalent to $4(6k) + 1$, and so it belongs to the congruence class ($1 \mod 4$). The form $24k + 3$ is equivalent to $8(3k) + 3$, and so it belongs to the congruence class ($3 \mod 8$). The form $24k + 5$ is equivalent to $4(6k + 1) + 1$, and so it belongs to the congruence class ($1 \mod 4$). The form $24k + 7$ is equivalent to $12(2k) + 7$, and so it belongs to the congruence class ($7 \mod 12$). The form $24k + 11$ is equivalent to $8(3k + 1) + 3$, and so it belongs to the congruence class ($3 \mod 8$). The form $24k + 13$ is equivalent to $4(6k + 3) + 1$, and so it belongs to the congruence class ($1 \mod 4$). The form $24k + 17$ is equivalent to $4(6k + 4) + 1$, and so it belongs to the congruence class ($1 \mod 4$). The form $24k + 19$ is equivalent to $8(3k + 2) + 3$, and so it belongs to the congruence class ($3 \mod 8$). And then we have the form $24k + 23$ in the congruence class ($23 \mod 24$). □

Exercise 23. *Let G be the subset of $M_2(\mathbb{C})$ consisting of the four matrices*

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}.$$

Prove that G is a multiplicative group isomorphic to the additive group of congruence classes $\mathbb{Z}/4\mathbb{Z}$.

Proof. The first matrix is the identity matrix. We observe that

$$\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},$$
$$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},$$
$$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}.$$

The multiplication in G is commutative. Let $f : G \to \mathbb{Z}/4\mathbb{Z}$ be a function defined by

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \rightsquigarrow 0 \mod 4,$$
$$\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \rightsquigarrow 1 \mod 4,$$
$$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} \rightsquigarrow 2 \mod 4,$$
$$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \rightsquigarrow 3 \mod 4.$$

It is checked that f is a homomorphism. Clearly f is a bijection. It follows that f is an isomorphism and $G \cong \mathbb{Z}/4\mathbb{Z}$. □

2.2 Linear Congruences

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

Exercise 2. *Find all Proofs of the congruence* $12x \equiv 3 \mod 45$.

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

Exercise 3. *Find all Proofs of the congruence* $28x \equiv 35 \mod 42$.

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

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* $0 \leq b \leq 2$.

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

$$\begin{aligned}
0 &\equiv 0 \cdot 3 + 0 \cdot 4 \mod 12, & 6 &\equiv 2 \cdot 3 + 0 \cdot 4 \mod 12,\\
1 &\equiv 3 \cdot 3 + 1 \cdot 4 \mod 12, & 7 &\equiv 1 \cdot 3 + 1 \cdot 4 \mod 12,\\
2 &\equiv 3 \cdot 3 + 2 \cdot 4 \mod 12, & 8 &\equiv 0 \cdot 3 + 2 \cdot 4 \mod 12,\\
3 &\equiv 1 \cdot 3 + 0 \cdot 4 \mod 12, & 9 &\equiv 3 \cdot 3 + 0 \cdot 4 \mod 12,\\
4 &\equiv 0 \cdot 3 + 1 \cdot 4 \mod 12, & 10 &\equiv 2 \cdot 3 + 1 \cdot 4 \mod 12,\\
5 &\equiv 3 \cdot 3 + 2 \cdot 4 \mod 12, & 11 &\equiv 1 \cdot 3 + 2 \cdot 4 \mod 12.\square
\end{aligned}$$

Exercise 3 is a simple verification.

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

PROOF. 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.

PROOF. 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* $\varphi(m) = m - 1$.

PROOF. 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.*

PROOF. 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* $\varphi(n)$.

Proof. This becomes obvious once we write down the expressions

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

Since $m|n$, 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.*

Proof.

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

Proof. The relation is true for all n which are not divisible by 5. □

Exercise 11. *Let $f(n) = \varphi(n)/n$. Prove that $f(p^k) = f(p)$ for all primes p and all positive integers k.*

Proof. By Euler totient function, $f(p^k) = \dfrac{\varphi(p^k)}{p^k} = \left(1 - \dfrac{1}{p}\right) = \dfrac{\varphi(p)}{p} = f(p)$. □

2.4 Chinese Remainder Theorem

Exercise 1. *Find all Proofs of the system of congruences*

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

Proof. Since $\gcd(5, 6) = 1$ and $5 \equiv 4 \mod 1$, the system has a Proof. 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 Proof $u \equiv 5 \mod 6$. All Proofs 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 Proofs of the system of congruences*

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

Proof.

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

Proof. We simply need to find all Proofs 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 Proof is $u \equiv 0 \mod 5$. Therefore the Proof to the first two congruences is $1 + 15v$. Continuing with the third congruence, we find that the Proofs 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*.*

Proof. We simply need to find all Proofs to the following system of congruences:

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

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

Exercise 7. *Find all Proofs of the congruence*

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

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

$$\begin{aligned} 5x^3 - 93 &\equiv 0 \mod 3, \\ 5x^3 - 93 &\equiv 0 \mod 7, \\ 5x^3 - 93 &\equiv 0 \mod 11. \end{aligned}$$

Or equivalently,

$$\begin{aligned} 5x^3 &\equiv 0 \mod 3, \\ 5x^3 - 2 &\equiv 0 \mod 7, \\ 5x^3 + 5 &\equiv 0 \mod 11. \end{aligned}$$

It can be checked that these congruences have the Proofs

$$\begin{aligned} f(0) &\equiv 0 \mod 3, \\ f(3) &\equiv 0 \mod 7, \\ f(10) &\equiv 0 \mod 11. \end{aligned}$$

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

$$\begin{aligned} a &\equiv 0 \mod 3, \\ a &\equiv 3 \mod 7, \\ a &\equiv 10 \mod 11. \end{aligned}$$

From the first congruence, we have $a = 3u$ for some integer u. Using this in the second congruence, we have $a = 3u \equiv 3 \mod 7$, which has the Proof $u \equiv 1 \mod 7$, and so $a = 3u = 3(1 + 7v) = 3 + 21v$. Using this in the third congruence, we have $a = 3 + 21v \equiv 10 \mod 11$ or equivalently $21v \equiv 7 \mod 11$, which has the Proof $4 \mod 11$, and so $a = 3 + 21(4 + 11w)$ or equivalently $a = 87 + 231\mathbb{Z}$. It is checked that $f(87) \equiv 0 \mod 231$. □

Exercise 8. *(Bhaskara, sixth century) A basket contains n eggs. If the eggs are removed* $2, 3, 4, 5,$ *or* 6 *at a time, then the number of eggs that remain in the basket is* $1, 2, 3, 4,$ *or* 5 *respectively. If the eggs are removed* 7 *at a time, then no eggs remain. What is the smallest number n of eggs that could have been in the basket at the start of this procedure?*

Proof. The given conditions imply that

$$\begin{aligned} n &\equiv 1 \mod 2, \\ n &\equiv 2 \mod 3, \\ n &\equiv 3 \mod 4, \\ n &\equiv 4 \mod 5, \\ n &\equiv 5 \mod 6. \end{aligned}$$

Then we solve for the smallest n satisfying all the above congruences.

2.5 Euler's Theorem and Fermat's Theorem

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

Proof. Since $1024 = 2^{10}$, the Euler totient function yields $\varphi(1024) = 2^{10}\left(1 - \frac{1}{2}\right) = 512$. By Theorem 2.12, it follows that $3^{512} \equiv 1 \mod 1024$. □

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

Proof. 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.

Proof. We observe that

$$\begin{aligned} 2^1 &\equiv 2 \mod 3, \\ 2^2 &\equiv 1 \mod 3, \end{aligned}$$

so that $\mathrm{ord}_3(2) = 2$. Similarly, we compute $\mathrm{ord}_5(2) = 4$, $\mathrm{ord}_7(2) = 3$, $\mathrm{ord}_{11}(2) = 10$, $\mathrm{ord}_{13}(12)$, $\mathrm{ord}_{17}(2) = 8$ and $\mathrm{ord}_{19}(2) = 18$. We need not compute all powers of 2 to find the order, we only compute the powers whose exponents divide the modulo minus one. For instance, to find $\mathrm{ord}_{17}(2)$, we compute

$$\begin{aligned} 2^2 &\equiv 4 \mod 17, \\ 2^4 &\equiv 16 \mod 17, \\ 2^8 &\equiv 1 \mod 17, \end{aligned}$$

so that the order of 2 modulo 17 is 8.

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

Proof. The divisors of 6 are $1, 2, 3$, and 6. We compute

$$10^1 \equiv 10 \mod 7,$$

$$
\begin{aligned}
10^2 &\equiv 9 \mod 7,\\
10^3 &\equiv 6 \mod 7,\\
10^6 &\equiv 1 \mod 7,
\end{aligned}
$$

so that the order of 10 modulo 7 is 6. Clearly 10 is a primitive root modulo 7. □

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?*

Proof. 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.... The numbers $r_1, \ldots, r_6$ appear as remainders in the long division of 1 by 7. □

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

Proof. The order of 10 modulo 13 must divide $\varphi(13) = 12$. Thus, it could be $2, 4, 6$, or 12. We compute

$$
\begin{aligned}
10^2 &\equiv 100 \equiv 9 \mod 13,\\
10^4 &\equiv 9^2 \equiv 3 \mod 13,\\
10^6 &\equiv 9^3 \equiv 3 \cdot 9 \equiv 1 \mod 13,
\end{aligned}
$$

so that $\mathrm{ord}_{13}(10) = 6$. 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 $2^{n+1} \mod p$.*

Proof. 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 $1 \leq k < 2^{n+1}$ such that $a^k \equiv 1 \mod p$. Therefore, a has order $2^{n+1} \mod p$. □

2.6 Pseudoprimes and Carmichael Numbers

Exercise 1. *Prove that 589 is composite by computing the least nonnegative residue of $2^{588} \mod 589$.*

Proof. We observe that $588 = 7 \cdot 7 \cdot 12$ so that

$$
\begin{aligned}
2^{588} &\equiv 2^7 \cdot 2^7 \cdot 2^{12} \mod 589\\
&\equiv 128 \cdot 128 \cdot 562 \mod 589\\
&\equiv 0 \mod 589.
\end{aligned}
$$

Therefore, 589 is composite. □

Exercise 2. *Let n be an odd integer, $n \geq 3$. Prove that there exists a nonnegative integer u such that $n + u^2 = (u+1)^2$. Prove that n is composite if and only if there exist nonnegative integers u and v such that $v > u + 1$ and $n + u^2 = v^2$. Use this method to factor 589.*

Proof.

Exercise 3. *Prove that* 645 *is a pseudoprime to base* 2.

Proof. We see that $2^{12} \equiv 226 \mod 645$ so that $2^{25} \equiv 2 \cdot (2^{12})^2 \equiv 242 \mod 645$. Now,

$$\begin{aligned} 2^{50} &\equiv (2^{25})^2 \equiv 514 \mod 645, \\ 2^{100} &\equiv (2^{50})^2 \equiv 391 \mod 645, \\ 2^{200} &\equiv (2^{100})^2 \equiv 16 \mod 645, \\ 2^{600} &\equiv 2^{200} \cdot 2^{200} \cdot 2^{200} \equiv 226 \mod 645. \end{aligned}$$

Therefore, $2^{644} \equiv 2^{600} \cdot 2^{25} \cdot 2^{12} \cdot 2^7 \equiv 1 \mod 645$. So, 645 is a pseudoprime to base 2. □

Exercise 4. *Prove that* 1729 *is a pseudoprime to bases* 2, 3, *and* 5.

Proof. As in Exercise 3, it is checked that $2^{1728} \equiv 1 \mod 1729$, $3^{1728} \equiv 1 \mod 1729$, and $5^{1728} \equiv 1 \mod 1729$. □

Exercise 5. *Prove that* 1105 *is a Carmichael number.*

Proof. Let b be an integer relatively prime to 1105. We need to show that $b^{1104} \equiv 1 \mod 1105$. We observe that $1105 = 5 \cdot 13 \cdot 17$. By Fermat's little theorem, we obtain

$$\begin{aligned} b^4 &\equiv 1 \mod 5 &\quad \text{so that} \quad b^{1104} &\equiv (b^4)^{276} \mod 5, \\ b^{12} &\equiv 1 \mod 13 &\quad \text{so that} \quad b^{1104} &\equiv (b^{12})^{92} \mod 13, \\ b^{16} &\equiv 1 \mod 17 &\quad \text{so that} \quad b^{1104} &\equiv (b^{16})^{69} \mod 17. \end{aligned}$$

It follows that $b^{1104} \equiv 1 \mod 1105$. So, 1105 is a Carmichael number. □

Exercise 6. *Let n be a product of distinct primes. Prove that if $p-1$ divides $n-1$ for every prime p that divides n, then n is a Carmichael number.*

Proof. This Proof is simply a generalization of Exercise 5. Let $n = \prod_{i=0}^{k} p_i$ where $p_i \neq p_j$ when $i \neq j$. Let b be an integer relatively prime to n. By Fermat's little theorem,

$$b^{p_i-1} \equiv 1 \mod p_i \qquad \text{so that} \qquad b^{n-1} \equiv (b^{p_i-1})^{(n-1)/(p_i-1)} \equiv 1 \mod p_i,$$

for each $0 \leq i \leq k$, and $(n-1)/(p_i-1)$ is an integer (since $p_i - 1$ divides $n-1$). It follows that $b^{n-1} \equiv 1 \mod n$. So, n is a Carmichael number. □

Exercise 7. *Prove that* 6601 *is a Carmichael number.*

Proof. Prime factorization of 6601 yields $6601 = 7 \cdot 23 \cdot 41$. It is checked that $6, 22$, and 40 divide 6600. By Exercise 7, it follows that 6601 is a Carmichael number. □

2.7 Public Key Cryptography

Exercise 1. *Consider the secret key cryptosystem constructed from the prime $p = 947$ and the encoding key $e = 167$. Encipher the plaintext $P = 2$. Find a decrypting key and decipher the ciphertext $C = 3$.*

PROOF. Since $0 < P < 947$ and $\gcd(167, 946) = 1$, we compute

$$C \equiv 2^{167} \equiv 172 \mod 947,$$

so that $C = 172$ is the ciphertext. Since $167 \cdot 465 \equiv 1 \mod 947$, it follows that $d = 465$ is a decrypting key. We see that

$$P \equiv C^d \equiv 3^{465} \equiv 376 \mod 947,$$

so that $P = 376$ is the plaintext. □

EXERCISE 2. *Consider the primes $p = 53$ and $q = 61$. Let $m = pq$. Prove that $e = 7$ is relatively prime to $\varphi(m)$. Find a positive integer d such that $ed \equiv 1 \mod \varphi(m)$.*

PROOF. Euler totient function yields $\varphi(m) = 3120$. We see that $3120 = 2^4 \cdot 3 \cdot 5 \cdot 13$. Since 7 is not a prime factor of 3120, it follows that $e = 7$ is relatively prime to $\varphi(m)$. We need to find a positive integer d such that $7 \cdot d \equiv 1 \mod 3120$. We observe that $d = 1783$ satisfies the condition. □

EXERCISE 3. *The integer 6059 is the product of two distinct primes, and $\varphi(6059) = 5904$. Use Theorem 2.19 to compute the prime divisors of 6059.*

PROOF. By Theorem 2.19, the prime divisors of 6059 are roots of the quadratic equation

$$x^2 - 156x + 6059 = 0.$$

On solving, we see that 73 and 83 are its roots. It can be checked that $73 \cdot 83 = 6059$. □

EXERCISE 4. *The probability that an integer chosen at random between 1 and n is relatively prime to n is $\varphi(n)/n$. Let $n = pq$, where p and q are two distinct primes greater than x. Prove that the probability that a randomly chosen positive integer up to x is relatively prime to n is greater than $(1 - 1/x)^2$. If $x = 200$, this probability is greater than 0.99.*

PROOF.

3 Primitive Roots and Quadratic Reciprocity

3.1 Polynomials and Primitive Roots

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

PROOF. 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.

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

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

PROOF. In Exercise 3 we proved that 2 is a primitive root of 101. Thus, $27 \equiv 2^k \mod 101$ has a unique Proof satisfying $0 \leq k \leq 99$. 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*?*

PROOF. By successive computation of $3^i \mod 101$ for $i \geq 1$ we find that $3^{100} \equiv 1 \mod 101$ and there is no $k \leq 100$ 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 Proofs of the congruence* $2^x \equiv 22 \mod 53$.

PROOF. 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* $k \geq 1$. *Find a primitive root modulo* 10. *Find a primitive root modulo* 50.

PROOF. 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 $k \geq 1$. 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*

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

Proof. 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 $i = 1, 2, \ldots, p-1$.*

Proof. By definition

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}.$$

Using the notation $v_p(m)$ to denote the exponent of the highest power of p that divides m,

$$\begin{aligned} v_p(\binom{p}{i}) &= v_p(p!) - v_p(i!) - v_p((p-i)!) \\ &= \sum_{j=1}^{p} v_p(j) - \sum_{j=1}^{i} v_p(j) - \sum_{j=1}^{p-i} v_p(j) \\ &= v_p(p) + \sum_{j=1}^{p-1} v_p(j) - \sum_{j=1}^{i} v_p(j) - \sum_{j=1}^{p-i} v_p(j) \\ &= 1, \end{aligned}$$

where we have used the facts that $v_p(p) = 1$, and p does not occur in the prime factorization of any number less than p and so, $v_p(m) = 0$ for all $m < p$. This is how all the summations vanish. Clearly, p divides $\binom{p}{i}$. □

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

Proof. 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 Proofs.

Proof. We see that $\text{ord}_7(9) = 3$ and the highest power of 7 which divides $9^3 - 1$ is 7. Suppose the given congruence has Proofs. 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 Proofs 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 Proofs of the congruence* $x^3 \equiv 8 \mod 19$.

Proof. 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 Proofs 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.*

Proof. 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

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

It is checked that the Proofs 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.*

Proof. Homomorphism is proved in the same way as in Exercise 5. Now, $(\mathbb{Z}/23\mathbb{Z})^\times = \{1, \ldots, 22\}$. The following table completely describes the function (for brevity we drop "modulo" with an understanding that all quantities are modulo 23).

$$\begin{array}{llll}
f(1) = 1, & f(7) = 21, & f(13) = 12, & f(19) = 5, \\
f(2) = 8, & f(8) = 6, & f(14) = 7, & f(20) = 19, \\
f(3) = 4, & f(9) = 16, & f(15) = 17, & f(21) = 15, \\
f(4) = 18, & f(10) = 11, & f(16) = 2, & f(22) = 22, \\
f(5) = 10, & f(11) = 20, & f(17) = 14, & \\
f(6) = 9, & f(12) = 3, & f(18) = 13. &
\end{array}$$

It is easily checked that f is both one-one and onto. Therefore, f is an isomorphism. □

3.4 Quadratic Residues

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

Proof. Since $\left(\frac{2}{47}\right) = 2^{(47-1)/2} = 1$, the congruence has a Proof. Since it is a quadratic equation modulo a prime, there are two Proofs (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 Proofs 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* $\left(\frac{7}{11}\right)$.

Proof. 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.*

Proof. Let $S = \{2, 4, 6, \ldots, p-1\}$. Then $-S = \{-(p-1), -(p-3), \ldots, -2\}$. We observe that $-(p-1) \equiv 1 \mod p$, $-(p-3) \equiv 3 \mod p$, ..., $-2 \equiv p-2 \mod p$. 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.*

Proof. By Theorem 3.14,

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

By Theorem 3.16,

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

It follows that

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

This gives all primes p for which -2 is a quadratic residue. □

Exercise 7. *Find all primes p for which 4 is a quadratic residue.*

Proof. By Theorem 3.16,

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

so that

$$\left(\frac{4}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/4}.$$

Any prime p satisfies either $1 \mod 4$ or $3 \mod 4$. Substituting these values in the above relation, we obtain that $\left(\frac{4}{p}\right) = 1$ in each case. It follows that 4 is a quadratic residue modulo every prime p. □

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?*

PROOF. 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. □

EXERCISE 11. *A binary quadratic form is a polynomial*

$$f(x, y) = ax^2 + bxy + cy^2, \qquad \textit{where } a, b, c \textit{ are integers.}$$

The discriminant of this form is the integer $d = b^2 - 4ac$. Show that

$$4af(x, y) = (2ax + by)^2 - dy^2.$$

PROOF. By expanding,

$$\begin{aligned}(2ax + by)^2 - dy^2 &= 4a^2x^2 + 4abxy + b^2y^2 - b^2y^2 - 4acy^2 \\ &= 4a(ax + bxy + cy^2) \\ &= 4af(x),\end{aligned}$$

which is what we wanted to show. □

EXERCISE 12.

3.5 Quadratic Reciprocity Law

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

PROOF. 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 4. *Prove that the congruence*

$$(x^2 - 2)(x^2 - 17)(x^2 - 34) \equiv 0 \mod p$$

has a Proof for every prime number p.

PROOF. It is easy to see that the given congruence has a Proof if at least one of the following congruences has a Proof:

$$x^2 - 2 \equiv 0 \mod p,$$

$$\begin{aligned} x^2 - 17 &\equiv 0 \mod p, \\ x^2 - 34 &\equiv 0 \mod p, \end{aligned}$$

which is the same as saying at least one of the Legendre symbols $\left(\frac{2}{p}\right)$, or $\left(\frac{17}{p}\right)$, or $\left(\frac{34}{p}\right)$ should evaluate to 1. Since the Legendre symbol is completely multiplicative,

$$\left(\frac{34}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{17}{p}\right)$$

If at least one of the Legendre symbols on the right hand side evaluate to 1, we are done. Otherwise both of the Legendre symbols evaluate to -1 so that $\left(\frac{34}{p}\right)$ evaluate to 1. In each case, at least one of the Legendre symbols always evaluates to 1. Therefore, the given congruence relation has a Proof for each prime p. □

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

PROOF. 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

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

□

EXERCISE 7. *Find all primes for which* -3 *is a quadratic residue.*

PROOF. Since the Legendre symbol is completely multiplicative,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right).$$

By Theorem 3.14,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4, \\ -1 & \text{if } p \equiv 3 \mod 4. \end{cases}$$

Using this relation and by Exercise 6, if $p \equiv 1 \mod 4$,

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

and if $p \equiv 3 \mod 4$,

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

Therefore, -3 is a quadratic residue modulo p if p satisfies one of the two following two conditions: (1) $p \equiv 1 \mod 4, p \equiv 1 \mod 3$, or (2) $p \equiv 3 \mod 4, p \equiv 1 \mod 3$. □

Exercises 8-9 are similar to what we have done thus far.

EXERCISE 11. *In Exercises* $11-17$ *we derive properties of the Jacobi symbol, which is a generalization of the Legendre symbol to composite moduli. Let* m *be an odd positive integer, and let*

$$m=\prod_{i=1}^{r} p_i^{k_i}$$

be the factorization of m *into the product of powers of distinct prime numbers. For any nonzero integer* a*, we define the Jacobi symbol* $\left(\frac{a}{m}\right)$ *as follows:*

$$\left(\frac{a}{m}\right)=\prod_{i=1}^{r}\left(\frac{a}{p_i}\right)^{k_i}.$$

(a) Prove that if $a \equiv b \mod m$*, then*

$$\left(\frac{a}{m}\right)=\left(\frac{b}{m}\right).$$

(b) For any integers a *and* b*, prove that*

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

(c) Prove that $\left(\frac{a}{m}\right)=0$ *if and only if* $(a,m)>1$.

PROOF. The idea is to reduce the Jacobi symbol to Legendre symbols whose properties we are already familiar with.

(a) Since $a \equiv b \mod m$, it follows that $a \equiv b \mod p_i$ for each prime factor p_i of m. Therefore, the following should be obvious:

$$\left(\frac{a}{m}\right)=\prod_{i=1}^{r}\left(\frac{a}{p_i}\right)^{k_i}=\prod_{i=1}^{r}\left(\frac{b}{p_i}\right)^{k_i}=\left(\frac{b}{m}\right).$$

(b) From the definition of Jacobi symbol and properties of Legendre symbol, it follows that,

$$\left(\frac{ab}{m}\right)=\prod_{i=1}^{r}\left(\frac{ab}{p_i}\right)^{k_i}=\prod_{i=1}^{r}\left(\frac{a}{p_i}\right)^{k_i}\left(\frac{b}{p_i}\right)^{k_i}=\prod_{i=1}^{r}\left(\frac{a}{p_i}\right)^{k_i}\prod_{i=1}^{r}\left(\frac{b}{p_i}\right)^{k_i}=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right).$$

(c) Suppose $\left(\frac{a}{m}\right)=0$. Clearly $\left(\frac{a}{p_i}\right)=0$ for some prime factor p_i of m. Since this is a Legendre symbol, it follows that p_i divides a. That is, p_i divides both a and m. It follows that $\gcd(a,m)>1$. Conversely, suppose $\gcd(a,m)>1$, that is, a and m have a common prime divisor (say p_j where $1\le j\le r$). Then

$$\left(\frac{a}{m}\right)=\prod_{i=1}^{r}\left(\frac{a}{p_i}\right)^{k_i}=\prod_{i=1}^{j-1}\left(\frac{a}{p_i}\right)^{k_i}\left(\frac{a}{p_j}\right)^{k_j}\prod_{i=j+1}^{r}\left(\frac{a}{p_i}\right)^{k_i}=0.$$

□

Exercise 12. *Compute the Jacobi symbol* $\left(\frac{38}{165}\right)$.

Proof. Prime factorization yields $38 = 2 \cdot 19$ and $165 = 3 \cdot 5 \cdot 11$. Therefore,

$$\left(\frac{38}{165}\right) = \left(\frac{2}{3}\right)\left(\frac{19}{3}\right)\left(\frac{2}{5}\right)\left(\frac{19}{5}\right)\left(\frac{2}{11}\right)\left(\frac{19}{11}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{3}\right)\left(\frac{2}{5}\right)\left(\frac{4}{5}\right)\left(\frac{2}{11}\right)\left(\frac{8}{11}\right)$$

Using the formula $\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p$ to compute $\left(\frac{2}{3}\right) = -1$, $\left(\frac{1}{3}\right) = 1$, $\left(\frac{2}{5}\right) = -1$, $\left(\frac{2}{11}\right) = -1$, it follows that

$$\left(\frac{38}{165}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{3}\right)\left(\frac{2}{5}\right)^3\left(\frac{2}{11}\right)^4 = 1.$$

□

Exercise 13. *Let m be an odd integer, and let $(a, m) = 1$. The integer a is called a quadratic residue modulo m if there exists an integer x such that*

$$x^2 \equiv a \mod m$$

and a quadratic nonresidue modulo m if this congruence has no Proof. Prove that if $\left(\frac{a}{m}\right) = -1$, then a is a quadratic nonresidue modulo m. Prove that a is not necessarily a quadratic residue modulo m if $\left(\frac{a}{m}\right) = 1$.

Proof. Let $m = \prod_{i=1}^{r} p_i^{k_i}$ be its prime factorization. Suppose a is a quadratic residue modulo m. That is, there is some integer x satisfying $x^2 \equiv a \mod m$. Then, $x^2 \equiv a \mod p_i$ for each $1 \leq i \leq r$ (because if m divides $x^2 - a$, then p_i also divides $x^2 - a$). Therefore, $\left(\frac{a}{p_i}\right) = 1$ for each p_i. But the given condition says

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{r}\left(\frac{a}{p_i}\right)^{k_i} = -1,$$

which is true only when $\left(\frac{a}{p_j}\right) = -1$ for some p_j where $1 \leq j \leq r$. This is absurd. It follows that a is a quadratic nonresidue modulo m. For the second part of the question, we consider $m = 21$ and $a = -1$. We observe that

$$\left(\frac{-1}{21}\right) = \left(\frac{-1}{3}\right)\left(\frac{-1}{7}\right) = (-1)(-1) = 1.$$

That is, -1 is a quadratic nonresidue modulo 3 and 7. Then -1 cannot be a quadratic residue modulo 21 (by the arguments used in the first part of the question). □

Exercise 14. *Let $m = p^k$, where p is an odd prime and $k \geq 1$. Prove that*

$$\frac{m-1}{2} \equiv \frac{k(p-1)}{2} \mod 2.$$

Proof. The proposition is trivially true when $k = 1$. So, we assume that $k \geq 2$. Then

$$m = ((p-1)+1)^k$$

$$= (p-1)^k + k(p-1)^{k-1} + \cdots + k(p-1) + 1$$
$$\frac{m-1}{2} = \frac{(p-1)^k}{2} + \frac{k(p-1)}{2}[(p-1)^{k-2} + \cdots + 1].$$

Since $k \geq 2$ and $p-1$ is even, it follows that $(p-1)^k/2$ is divisible by 2. Also, all powers of $p-1$ are divisible by 2. Therefore, taking modulo 2 on both sides yield

$$\frac{m-1}{2} \equiv \frac{k(p-1)}{2} \mod 2.\square$$

Exercise 15. *Let m be an odd positive integer with standard factorization $m = \prod_{i=1}^r p_i^{k_i}$. Prove that*

$$\frac{m-1}{2} \equiv \sum_{i=1}^r \frac{k_i(p_i-1)}{2} \mod 2.$$

Prove that

$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2}.$$

Proof. We shall prove the proposition by induction on r. The base case of $r=1$ reduces to what we proved in Exercise 14. Suppose the proposition holds for some $r-1 \in \mathbb{Z}, r-1 > 1$.

3.6 Quadratic Residues to Composite Moduli

Exercise 1. *Let $x_1 = 3$. Construct integers x_k such that $x_k^2 \equiv 2 \mod 7^k$ and $x_k \equiv x_{k-1} \mod 7^{k-1}$ for $k = 2, 3, 4$.*

Proof. Let $f(x) = x^2 - 2$. Then $f'(x) = 2x$. We see that $f(x_1) \equiv 0 \mod 7$ and $f'(x_1) \not\equiv 0 \mod 7$. By Hensel's lemma, there exists x_k for all $k \geq 2$ such that $x_k^2 \equiv 2 \mod 7^k$ and $x_k \equiv x_{k-1} \mod 7^{k-1}$. When $k=2$, we must have $x_2^2 \equiv 2 \mod 49$ and $x_2 \equiv 3 \mod 7$. It can be checked that $x_2 = 10$ satisfies the equations. When $k=3$, we must have $x_3^2 \equiv 2 \mod 343$ and $x_3 \equiv 10 \mod 49$. It can be checked that $x_3 = 108$ satisfies the equations. When $k=4$, we must have $x_4^2 \equiv 2 \mod 2401$ and $x_4 \equiv 108 \mod 343$. It can be checked that $x_4 = 2166$ satisfies the given equations. □

Exercise 2. *Let p be a prime, $p \neq 3$, and let a be an integer not divisible by p. Prove that if a is a cubic residue modulo p, then a is a cubic residue modulo p^k for every $k \geq 1$.*

Proof. Let $f(x) = x^3 - a$. Then $f'(x) = 3x^2$. If a is a cubic residue of p, there exists an integer x_1 such that $x_1 \not\equiv 0 \mod p$ and $x_1^3 \equiv a \mod p$. Then $x_1^2 \not\equiv 0 \mod p$ (since p is a prime), so that $f'(x_1) \not\equiv 0 \mod p$. By Hensel's lemma, there exists $x_k \in \mathbb{Z}$ such that $f(x_k) \equiv 0 \mod p^k$. Therefore, a is a cubic residue modulo p^k for every $k \geq 1$. □

Exercise 3. *Denote the derivative of the polynomial $f(x)$ by $D(f)(x) = f'(x)$. We define*

$$\begin{aligned} &D^{(0)}(f)(x) = f(x), \\ &D^{(k)}(f)(x) = D\left(D^{(k-1)}(f)\right)(x) \qquad \textit{for } k \geq 1. \end{aligned}$$

The polynomial $D^{(k)}(f)$ is called the kth derivative of f. Prove that if $f(x)$ is a polynomial with integer coefficients, then $D^{(k)}(f)(x) = 0$ if and only if the degree of $f(x)$ is at most $k-1$.

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial of degree n with $a_n \neq 0$, and $a_i \in \mathbb{Z}$ for all $0 \leq i \leq n$. Then $D^{(1)}(f)(x) = a_n n x^{n-1} + a_{n-1}(n-1)x^{n-2} + \cdots + a_1$. Following this manner, we can write $D^{(k)}(f)(x) = a_n n(n-1)\cdots(n-k+1)x^{n-k} + a_{n-1}(n-1)(n-2)\cdots(n-k)x^{n-k-1} + \cdots + a_k$. Suppose $D^{(k)}(f)(x) = 0$. Since $a_n \neq 0$, and $x^i \neq 0$ for any $i \in \mathbb{Z}$, we must have $n(n-1)\cdots(n-k+1) = 0$, and so n can be at most $n = k-1$. Conversely, suppose n is at most $k-1$, that is $n \leq k-1$. It is easy to see that $D^{(k)}(f)(x) = 0$ (equivalently, $D^{(k)}(f)(x)$ has no nonzero terms). □

Exercise 4. *Let $f(x)$ and $g(x)$ be polynomials. Prove the Leibniz formula*

$$D(f \cdot g)(x) = f(x) \cdot D(g)(x) + D(f)(x) \cdot g(x).$$

Proof. Let $f(x) = \sum_{i=0}^{m} a_i x^i$ and $g(x) = \sum_{j=0}^{n} b_j x^j$ be any two polynomials with $a_m \neq 0$ and $b_n \neq 0$. To make the result as general as it can be, the coefficients a_i, b_j are allowed to be from any ring R. Then the formal derivatives of f and g are given by

$$\begin{aligned} D(f)(x) &= a_m m x^{m-1} + a_{m-1}(m-1)x^{m-2} + \cdots + a_1, \\ D(g)(x) &= b_n n x^{n-1} + b_{n-1}(n-1)x^{n-2} + \cdots + b_1. \end{aligned}$$

Now, $f \cdot g = a_m b_n x^{m+n} + (a_m b_{n-1} + a_{m-1}b_n)x^{m+n-1} + \cdots + (a_1 b_0 + a_0 b_1)x + a_0 b_0$ so that

$$D(f \cdot g)(x) = a_m b_n (m+n)x^{m+n-1} + (a_m b_{n-1} + a_{m-1}b_n)(m+n-1)x^{m+n-2} + \cdots + (a_1 b_0 + a_0 b_1).$$

It becomes a simple computational endeavor to check that $f(x) \cdot D(g)(x) + D(f)(x) \cdot g(x)$ indeed equals the above expansion of $D(f \cdot g)(x)$. □

Exercise 5. *Let $f(x)$ be a polynomial of degree n. Prove Taylor's formula*

$$f(x+h) = \sum_{k=0}^{n} \frac{D^{(k)}(f)(x)}{k!} h^k.$$

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{k=0}^{n} a_k x^k$ so that $f(x+h) = a_n(x+h)^n + a_{n-1}(x+h)^{n-1} + \cdots + a_0 = \sum_{k=0}^{n} a_k (x+h)^k$. We want to prove that

$$f(x+h) = f(x) + f'(x)h + \frac{f''(x)}{2!}h^2 + \cdots + \frac{f^{(n)}(x)}{n!}h^n,$$

where we have used the familiar symbols borrowed from calculus, thereby keeping in mind that these (formal) derivatives are different from the ones we encounter in calculus where they are defined in terms of limits. We can write

$$f^{(k)}(x) = \left[\binom{n}{k} a_n x^{n-k} + \binom{n-1}{k} a_{n-1} x^{n-k-1} + \cdots + \binom{k}{k} a_k\right] k!.$$

Simply expanding the binomial coefficients yield the form of derivatives we are familiar with. By binomial theorem, we obtain

$$f(x+h) = a_n(x+h)^n + a_{n-1}(x+h)^{n-1} + a_{n-2}(x+h)^{n-2} + \cdots + a_1(x+h) + a_0$$

$$
\begin{aligned}
&= \left[a_0x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0\right] + \\
&\quad \left[na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1\right] h + \\
&\quad \left[\binom{n}{2}a_nx^{n-2} + \binom{n}{2}a_{n-1}x^{n-3} + \cdots + \binom{n}{2}a_2\right] h^2 + \\
&\quad \cdots \\
&\quad \cdots \\
&\quad \left[\binom{n}{n-1}a_nx\right] h^{n-1} + \\
&\quad \left[\binom{n}{n}a_n\right] h^n \\
&= f(x) + f'(x)h + \frac{f''(x)}{2!}h^2 + \cdots + \frac{f^n(x)}{n!}h^n \\
&= \sum_{k=0}^{n} \frac{D^{(k)}(f)(x)}{n!}h^k,
\end{aligned}
$$

where, in the final step, we get rid of the borrowed symbols. □

4 Fourier Analysis on Finite Abelian Groups

4.1 The Structure of Finite Abelian Groups

Exercise 1. *Let $G = \mathbb{Z}/12\mathbb{Z}$ be the additive group of congruence class modulo 12. Compute $G(2)$ and $G(3)$ and show explicitly that $G(2) \cong \mathbb{Z}/4\mathbb{Z}$, $G(3) \cong \mathbb{Z}/3\mathbb{Z}$, and*

$$\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

Proof. By computation, the orders of all the elements of $\mathbb{Z}/12\mathbb{Z}$ are given below

Element	Order	Element	Order
0	1	6	2
1	12	7	12
2	6	8	3
3	4	9	4
4	3	10	6
5	12	11	12,

so that $G(2) = \{0, 3, 6, 9\}$ and $G(3) = \{0, 4, 8\}$. Let $f : \mathbb{Z}/4\mathbb{Z} \to G(2)$ be a function defined by $f(x) = 3x$. Since there are only four elements in both the sets, it is easily checked that the function is one-one and onto. Indeed, $0 \rightsquigarrow 1$, $1 \rightsquigarrow 3$, $2 \rightsquigarrow 6$, and $3 \rightsquigarrow 9$. Homomorphism follows from the fact that $f(x+y) = 3(x+y) = 3x+3y = f(x)+f(y)$. Therefore, $G(2) \cong \mathbb{Z}/4\mathbb{Z}$. Let $g : \mathbb{Z}/3/Z \to G(3)$ be a function defined by $g(x) = 4x$. This function is also one-one and onto. Indeed, $0 \rightsquigarrow 0$, $1 \rightsquigarrow 4$, and $2 \rightsquigarrow 8$. This is also a homomorphism in the same way f was a homomorphism. Therefore $G(3) \cong \mathbb{Z}/3\mathbb{Z}$.

Exercise 2. *Let G be an abelian group, written additively, and let $G_1, \ldots, G_k$ be subgroups of G. Prove that $G_1 + \cdots + G_k$ is a subgroup of G.*

Proof. Since $0 \in G_1, \cdots, G_k$, it follows that $0 \in G_1 + \cdots + G_k$. Suppose $g \in G_1 \cdots + G_k$. Then there exist $g_i \in G_i$ for each $1 \leq i \leq k$ such that $\sum_{i=1}^k g_i = g$. Clearly $-g_i \in G_i$ for each $1 \leq i \leq k$ so that $-g = -\sum_{i=1}^k g_i \in G_1 + \cdots + G_k$. Suppose $x, y \in G_1 + \cdots + G_k$. Then there exist $x_i, y_i \in G_i$ for each $1 \leq i \leq k$ such that $\sum_{i=1}^k x_i = x$ and $\sum_{i=1}^k y_i = y$. Clearly $x + y = \sum_{i=1}^k x_i + \sum_{i=1}^k y_i = \sum_{i=1}^k (x_i + y_i) \in G_1 + \cdots + G_k$. It follows that $G_1 + \cdots + G_k$ is a subgroup of G. □

Exercise 3. *Let G be an abelian group, written additively, and let $G_1, \ldots, G_k$ be subgroups of G such that $G = G_1 + \cdots + G_k$. Prove that $|G| \leq |G_1| \cdots |G_k|$. Prove that $G = G_1 \oplus \cdots \oplus G_k$ if and only if $|G| = |G_1| \cdots |G_k|$.*

Exercise 4. *Let G be an abelian group, written additively, and let $G_1, \ldots, G_k$ be subgroups of G such that $G = G_1 + \cdots + G_k$. Prove that $G = G_1 \oplus \cdots \oplus G_k$ if and only if the only representation of 0 in the form $0 = g_1 + \cdots + g_k$ with $g_i \in G_i$ is $g_1 = \cdots = g_k = 0$.*

Proof. One direction is trivial. If $G = G_1 \oplus \cdots \oplus G_k$, then $0 = 0 + \cdots + 0$ is the only representation of 0 (because each representation is unique in direct sum). Conversely, suppose this is the only representation of 0. We shall prove that every $g \in G$ has a unique representation in the form $g = g_1 + \cdots + g_k$ with $g_i \in G_i$. Suppose there is another representation $g = g'_1 + \cdots + g'_k$ with $g'_i \in G_i$. Then, on subtraction, $g - g = 0 = g_1 - g'_1 + \cdots + g_k - g'_k$ with $g_i - g'_i \in G_k$. But the only representation of 0 is $0 = 0 + \cdots + 0$. It follows that $g_i = g'_i$ for each $1 \leq i \leq k$. It follows that $G = G_1 + \oplus \cdots \oplus G_k$. □

EXERCISE 5. *Let $G_1, \cdots, G_k$ be subgroups of an abelian group G such that $G = G_1 \oplus \cdots \oplus G_k$. Prove that $G \cong G_1 \times \cdots \times G_k$.*

EXERCISE 6. *Let G be an additive abelian group. For every prime number p, let $G(p)$ denote the set of all elements of G whose order is a power of p. Prove that $G(p)$ is a subgroup of G.*

PROOF. The identity $0 \in G(p)$. Because the order of 0 is $1 = p^0$. Suppose $g \in G(p)$. Let $\text{ord}(g) = p^r$. In other words, $p^r g = 0$ and $sg \neq 0$ for any $s < p^r$. Clearly $-p^r g = 0$ and $-sg \neq 0$ for any $s < p^r$. Thus, $\text{ord}(-g) = p^r$ and $-g \in G(p)$. Let $x, y \in G(p)$. Let $\text{ord}(x) = p^u$ and $\text{ord}(y) = p^v$. Then $p^u x = 0, p^v y = 0$ but $s_1 x \neq 0, s_2 y \neq 0$ for all $s_1 < p^u, s_2 < p^v$.

EXERCISE 7. *Let $f : G \to H$ be a group homomorphism, and let $g \in G$. Prove that the order of $f(g)$ in H divides the order of g in G. Prove that if G is a p-group and f is surjective , then H is a p-group.*

4.2 Characters of Finite Abelian Groups

EXERCISE 1. *Let C_2 be the cyclic group of order 2.*

(a) Compute the character table for C_2.

(b) Compute the character table for the group $C_2 \times C_2$.

PROOF.

(a) We have, $C_2 = \{0, 1\}$, and $\widehat{C_2} = \{\psi_a : a = 0, 1\}$ where

$$\psi_a(j) = e^{\frac{2\pi iaj}{2}} = e^{\pi iaj} \qquad \text{for } j \in C_2.$$

We have the character table

	0	1
ψ_0	1	1
ψ_1	1	-1

(b)

EXERCISE 2. *Compute the character table for the cyclic group of order* 6.

PROOF. We have, $C_6 = \{0, 1, \ldots, 5\}$, and $\widehat{C_6} = \{\psi_a : a = 0, 1, \ldots, 5\}$ where

$$\psi_a(j) = e^{\frac{2\pi iaj}{6}} = e^{\frac{\pi iaj}{3}} \qquad \text{for } j \in C_6.$$

We have the character table

	0	1	2	3	4	5
ψ_0	1	1	1	1	1	1
ψ_1	1	$e^{\frac{\pi i}{3}}$	$e^{\frac{2\pi i}{3}}$	$e^{\pi i}$	$e^{\frac{4\pi i}{3}}$	$e^{\frac{5\pi i}{3}}$
ψ_2	1	$e^{\frac{2\pi i}{3}}$	$e^{\frac{4\pi i}{3}}$	1	$e^{\frac{2\pi i}{3}}$	$e^{\frac{4\pi i}{3}}$
ψ_3	1	$e^{\pi i}$	1	$e^{\pi i}$	1	$e^{\pi i}$
ψ_4	1	$e^{\frac{4\pi i}{3}}$	$e^{\frac{2\pi i}{3}}$	1	$e^{\frac{4\pi i}{3}}$	$e^{\frac{2\pi i}{3}}$
ψ_5	1	$e^{\frac{5\pi i}{3}}$	$e^{\frac{4\pi i}{3}}$	$e^{\pi i}$	$e^{\frac{2\pi i}{3}}$	$e^{\frac{\pi i}{3}}$

□

EXERCISE 3. *Let G be a finite cyclic group of order n. Define the characters ψ_a on G by* (4.1)*. Prove that*

(a) $\psi_a\psi_b = \psi_{a+b}$*,*

(b) $\psi_a^{-1} = \psi_{-a}$*,*

(c) $\psi_a = \psi_b$ *if and only if* $a \equiv b \mod n$*.*

PROOF. By (4.1),

$$\psi_a(jg_0) = e^{2\pi iaj/n} \qquad \text{for } a \in \mathbb{Z}.$$

(a) For $a, b \in \mathbb{Z}$, we obtain

$$\psi_a\psi_b(jg_0) = \psi_a(jg_0)\psi_b(jg_0) = e^{2\pi iaj/n}e^{2\pi ibj/n} = e^{2\pi i(a+b)j/n} = \psi_{a+b}(jg_0).$$

(b) For $a \in \mathbb{Z}$, we obtain

$$\psi_a^{-1}(jg_0) = \psi_a(-jg_0) = e^{2\pi i(-a)j/n} = \psi_{-a}(jg_0).$$

(c) For $a, b \in \mathbb{Z}$, we obtain

$$\psi_a(jg_0) = \psi_b(jg_0) \iff e^{2\pi iaj/n} = e^{2\pi ibj/n} \iff a \equiv b \mod n$$

□

EXERCISE 4. *Prove that if G is cyclic and $g \in G$, $g \neq 0$, then $\psi_1(g) \neq 1$.*

PROOF. Let $G = \{jg_0 : j = 0, 1, \ldots, n-1\}$. By (4.1),

$$\psi_1(jg_0) = e^{2\pi ij/n}.$$

Since $g \neq 0$, it follows that $j \neq 0$. But the nth roots of unity form vertices of a regular n-gon and there is only one vertex at 1 which occurs when $j = 0$. Consequently, $\psi_1(g) \neq 1$. □

EXERCISE 5. *Prove that the map Ψ defined by* 4.3 *is a one-to-one homomorphism.*

EXERCISE 6. *Consider the map* $\langle , \rangle : G \times \widehat{G} \to C^\times$ *defined by*

$$\langle g, \chi \rangle = \chi(g).$$

Prove that

$$\langle g + g', \chi \rangle = \langle g, \chi \rangle \langle g', \chi \rangle \qquad \text{and} \qquad \langle g, \chi\chi' \rangle = \langle g, \chi \rangle \langle g, \chi' \rangle$$

for all $g, g' \in G$ *and* $\chi, \chi' \in \widehat{G}$.

PROOF. Let $g, g' \in G$. Let $\chi, \chi' \in \widehat{G}$. Then

$$\langle g + g', \chi \rangle = \chi(g + g') = \chi(g)\chi(g') = \langle g, \chi \rangle \langle g', \chi \rangle,$$

and

$$\langle g, \chi\chi' \rangle = \chi\chi'(g) = \chi(g)\chi'(g) = \langle g, \chi \rangle \langle g'\chi \rangle.$$

□

EXERCISE 7. *Let* $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. *For integers* a *and* b, *we define the function* $\psi_{a,b}$ *on* G *by*

$$\psi_{a,b}(x + m\mathbb{Z}, y + m\mathbb{Z}) = e^{2\pi i(ax+by)/m} = e_m(ax + by).$$

(a) *Prove that* $\psi_{a,b}$ *is well-defined.*

(b) *Prove that* $\psi_{a,b} = \psi_{c,d}$ *if and only if* $a \equiv c \mod m$ *and* $b \equiv d \mod m$.

(c) *Prove that* $\psi_{a,b}$ *is a character of the group* G.

(d) *Prove that* $\widehat{G} = \{\psi_{a,b} : a, b = 0, 1, \ldots, m-1\}$.

PROOF.

(a) Let $u \in \mathbb{Z}$. That $\psi_{a,b}$ is well-defined is obvious from the following

$$\begin{aligned} \psi_{a,b}(x + mu, y + mu) &= e^{2\pi i(ax+amu+by+bmu)/m} \\ &= e^{2\pi i(ax+by)/m} \cdot e^{2\pi iu(a+b)} \\ &= e^{2\pi i(ax+by)/m}, \end{aligned}$$

so that $\psi_{a,b}(x + mu, y + mu)$ does not depend on the choice of u.

(b) Suppose $\psi_{a,b} = \psi_{c,d}$ for $a, b, c, d \in \mathbb{Z}$. Then

$$e^{2\pi i(ax+by)/m} = e^{2\pi i(cx+dy)/m} \iff e^{2\pi iax/m} e^{2\pi iby/m} = e^{2\pi icx/m} e^{2\pi idy/m}.$$

Since the above equality is true for all values of x and y, we must have

$$e^{2\pi iax/m} = e^{2\pi icx/m} \qquad \text{and} \qquad e^{2\pi iby/m} = e^{2\pi idy/m}.$$

It follows that $2\pi ix(a-b)/m = 2\pi ixu$, that is, $a = b + mu$. Therefore, $a \equiv b \mod m$. Likewise, $b \equiv d \mod n$. The other direction follows trivially.

(c) We shall prove that $\psi_{a,b} : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}^\times$ is a homomorphism. Let $(x, y), (x', y') \in \mathbb{Z}/m\mathbb{Z}$. By definition of $\psi_{a,b}$, it follows that

$$\begin{aligned}\psi_{a,b}(x + x' + m\mathbb{Z}, y + y' + m\mathbb{Z}) &= e^{2\pi i[a(x+x')+b(y+y')]/m} \\ &= e^{2\pi i(ax+by)/m+2\pi i(ax'+by')/m} \\ &= e^{2\pi i(ax+by)/m} e^{2\pi i(ax'+by')/m} \\ &= \psi_{a,b}(x + m\mathbb{Z}, y + m\mathbb{Z})\psi_{a,b}(x' + m\mathbb{Z}, y' + m\mathbb{Z})\end{aligned}$$

(d) By Theorem 4.5, $G \cong \widehat{G}$. If we could find a set S which contains characters of G such that $|S| = |G|$, then we can conclude that $S = \widehat{G}$. We define

$$S \coloneqq \{\psi_{a,b} : a, b = 0, 1, \ldots, m - 1\}.$$

In (c), we proved that $\psi_{a,b}$ is a character of G. From (b), each $\psi_{a,b}$ is unique for $a, b = 0, 1, \ldots, m - 1$. It follows that $|S| = m^2 = |G|$. It follows that $\widehat{G} = \{\psi_{a,b} : a, b = 0, 1, \ldots, m - 1\}$. □

Exercise 8. *Let p be a prime number, and let $G = (\mathbb{Z}/p\mathbb{Z})^\times$ be the multiplicative group of units in the field $\mathbb{Z}/p\mathbb{Z}$. Let g be a primitive root modulo p. For every integer a, define the function $\chi_a : G \to C^\times$ as follows: If $(x, p) = 1$ and $x \equiv g^y \mod p$, then*

$$\chi_a(x + p\mathbb{Z}) = e^{2\pi ay/(p-1)} = e_{p-1}(ay).$$

(a) Prove that χ_a is a character, that is, $\chi_a \in \widehat{G}$.

(b) Prove that $\chi_a = \chi_b$ if and only if $a \equiv b \mod p - 1$.

(c) Prove that $\widehat{G} = \{\chi_a : a = 0, 1, \ldots, p - 2\}$.

Proof.

(a) We shall prove that $\chi_a : G \to \mathbb{C}^\times$ is a homomorphism. Let $\gcd(x, p) = 1$ and $x \equiv g^y \mod p$. Let $\gcd(x', p) = 1$ and $x' \equiv g^{y'} \mod p$.

Exercise 10. *Let G be a finite abelian group and $G^r = \{rg : g \in G\}$. Let $[G : G^r]$ be the index of the subgroup G^r in G. Prove that*

$$\sum_{\chi \in \widehat{G_r}} \chi(a) = \begin{cases} [G : G^r] & \text{if } a \in G^r \\ 0 & \text{if } a \notin G^r. \end{cases}$$

Proof. We consider the quotient group G/G^r. By Lagrange's theorem, $|G/G^r| = [G : G^r]$. By Theorem 4.5, $G_r = G/G^r \cong \widehat{G/G^r}$. Thus, $|\widehat{G_r}| = |\widehat{G/G^r}| = [G : G^r]$. Applying the orthogonality relations, we obtain the formula. □

4.3 Elementary Fourier Analysis

In these exercises, G is a finite abelian group.

Exercise 1. *Let $f, g \in L^2(G)$. Prove that*

$$(g, f) = \overline{(f, g)}.$$

Proof. By definition of inner product on $L^2(G)$, we obtain

$$(g, f) = \int_G g\overline{f} = \sum_{x \in G} g(x)\overline{f(x)} = \overline{\sum_{x \in G} f(x)\overline{g(x)}} = \overline{\int_G f\overline{g}} = \overline{(f, g)}.$$

□

Exercise 2. *Let $f \in L^2(G)$. Prove that if $c \in L^2(\widehat{G})$ and $f = (1/n)\sum_{\chi \in \widehat{G}} c(\chi)\chi$, then $c(\chi) = \widehat{f}(\chi)$.*

Proof. By a consequence of the orthogonality relations (Thoerem 4.7),

$$(\chi_1, \chi_2) = \begin{cases} n & \text{if } \chi_1 = \chi_2 \\ 0 & \text{if } \chi_2 \neq \chi_2. \end{cases}$$

That is, $\widehat{G} = \{\chi_1, \dots, \chi_n\}$ is an orthogonal set. Consequently, $\widehat{G}$ is linearly independent. But $|\widehat{G}| = n = \dim L^2(G)$. It follows that $\widehat{G}$ is a basis for $L^2(G)$. The first part of the proof of Theorem 4.8 establishes the Fourier series of f as

$$f = \frac{1}{n}\sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi.$$

Since $\widehat{G}$ is a basis, this representation must be unique so that $c(\chi) = \widehat{f}(\chi)$. □

Exercise 3. *Prove that the Haar measure on G is unique, that is, there exists a unique function μ on the subsets of G such that μ is additive, translation invariant, and $\mu(G) = n$.*

Proof. Let μ be a function on subsets of G such that μ is additive, translation invariant, and $\mu(G) = n$. We shall prove that μ is the Haar measure, that is, $\mu(U) = |U|$ for any $U \subset G$. Let $U = \{0\}$. Then for any $a \in G$, by translation invariance, we must have $\mu(U) = \mu(a + U)$. That is, $\mu(\{0\}) = \mu(\{a\})$. Indeed, for any $a, b \in G$, we have $\mu(\{a\}) = \mu(\{b\})$. By additivity,

$$\mu(G) = \mu(\bigcup_{a \in G} \{a\}) = \sum_{a \in G} \mu(\{a\}) = n.$$

But $|G| = n$. It follows that $\mu(\{a\}) = 1$. Again, by additivity, for any $U \subset G$,

$$\mu(U) = \sum_{a \in U} 1 = |U|,$$

which is the Haar measure. □

Exercise 4. *Let $U : L^2(G) \to L^2(\widehat{G})$ be a linear transformation such that $U(\delta_a)(\chi) = \overline{\chi}(a)$ for all $\chi \in \widehat{G}$. Prove that U is the Fourier transform, that is, $U(f) = \widehat{f}$ for all $f \in L^2(G)$.*

Exercise 5. *(Cauchy-Schwarz inequality) Let $f, g \in L^2(G)$. Prove that*

$$|(f, g)| \leq ||f||_2||g||_2.$$

Exercise 6. *Prove that if $f, g \in L^2(G)$, then*

$$||f + g||_2 \le ||f||_2 + ||g||_2.$$

Exercise 7. *Let $\chi_1, \chi_2 \in \widehat{G}$. Prove that*

$$\widehat{\chi_1}(\chi_2) = \begin{cases} n & \text{if } \chi_1 = \chi_2 \\ 0 & \text{if } \chi_1 \neq \chi_2. \end{cases}$$

Exercise 10. *For functions $f_1, f_2 \in L^2(G)$, we define the convolution $f_1 * f_2 \in L^2(G)$ by*

$$f_1 * f_2(a) = \int_G f_1(a - x) f_2(x) dx = \sum_{a \in G} f_1(a - x) f_2(x).$$

(a) Prove that

$$f_1 * f_2(a) = \sum_{x+y=a} f_1(x) f_2(y).$$

(b) Prove that convolution is commutative, that is,

$$f_1 * f_2 = f_2 * f_1.$$

(c) Prove that convolution is associative, that is,

$$(f_1 * f_2) * f_3 = f_1 * (f_2 * f_3).$$

(d) Prove that, if $f_1, \ldots, f_k \in L^2(G)$, then

$$f_1 * \cdots * f_k(a) = \sum_{x_1 + \cdots + x_k = a} f_1(x_1) \cdots f_k(x_k)$$

Proof.

(a) Let $a - x = y$. Since the summation is over the group,

$$f_1 * f_2(a) = \sum_{a \in G} f_1(a - x) f_2(x) = \sum_{x+y=a} f_1(y) f_2(x).$$

The above expression is symmetric in x and y (both of them are only dummy variables), so we may interchange them. It follows that

$$f_1 * f_2(a) = \sum_{x+y=a} f_1(x) f_2(y).$$

(b)

(c) By definition of convolution,

$$\begin{aligned}(f_1 * f_2) * f_3(a) &= \sum_{u+z=a} f_1 * f_2(u) f_3(z) \\ &= \sum_{u+z=a} \left(\sum_{x+y=u} f_1(x) f_2(y) \right) f_3(z) \\ &= \sum_{x+y+z=a} f_1(x) f_2(y) f_3(z).\end{aligned}$$

Likewise, it is checked that

$$f_1 * (f_2 * f_3)(a) = \sum_{x+y+z=a} f_1(x) f_2(y) f_3(z).$$

The associativity follows.

(d) Since convolution is associative, we can drop the parenthesis. It is easy to see that the proposition follows by induction. Indeed, we have already proved the base case. Proving $P(k) \implies P(k+1)$ follows almost exactly the same way as the proof of associativity in (c). □

Exercise 11. *Let $\chi \in \widehat{G}$. Prove that*

$$\underbrace{\chi * \cdots * \chi}_{k \ times}(a) = \sum_{x_1+x_2+\cdots+x_k=a} \chi(x_1 + x_2 + \cdots + x_k).$$

Proof. By Exercise 10 (d),

$$\begin{aligned}\underbrace{\chi * \cdots * \chi}_{k \text{ times}}(a) &= \sum_{x_1+x_2+\cdots+x_k=a} \chi(x_1)\chi(x_2)\cdots\chi(x_k) \\ &= \sum_{x_1+x_2+\cdots+x_k=a} \chi(x_1 + x_2 + \cdots + x_k),\end{aligned}$$

where we have used the fact that χ is a homomorphism. □

Exercise 12. *Let p be a prime number, and define $l_p \in L^2(\mathbb{Z}/p\mathbb{Z})$ by*

$$l_p(a + p\mathbb{Z}) = \left(\frac{a}{p}\right),$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. Prove that

$$\underbrace{l_p * \cdots * l_p}_{k \ times}(a + p\mathbb{Z}) = \sum_{\substack{x_1+x_2+\cdots+x_k=a \\ 1 \le x_i \le p-1}} \left(\frac{x_1 x_2 \cdots x_k}{p}\right).$$

Proof. By Exercise 10 (d),

$$\underbrace{l_p * \cdots * l_p}_{k \text{ times}}(a + p\mathbb{Z}) = \sum_{\substack{x_1+x_2+\cdots+x_k=a \\ 1 \le x_i \le p-1}} l_p(x_1) l_p(x_2) \cdots l_p(x_k)$$

$$
\begin{aligned}
&= \sum_{\substack{x_1+x_2+\cdots+x_k=a \\ 1\le x_i\le p-1}} \left(\frac{x_1}{p}\right)\left(\frac{x_2}{p}\right)\cdots\left(\frac{x_k}{p}\right) \\
&= \sum_{\substack{x_1+x_2+\cdots+x_k=a \\ 1\le x_i\le p-1}} \left(\frac{x_1x_2\cdots x_k}{p}\right).
\end{aligned}
$$

4.4 Poisson Summation

4.5 Trace Formula on Finite Abelian Groups

In these exercises, G is a finite abelian group of order n.

Exercise 1. *Let $A = (a_{ij})$ and $B = (b_{ij})$ be $n \times n$ matrices. Prove that $tr(AB) = tr(BA)$.*

Proof. From the definition of the multiplication of matrices,

$$\operatorname{tr}(AB) = \sum_{i=1}^{n}(AB)_{ii} = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}b_{ki} = \sum_{k=1}^{n}\sum_{i=1}^{n} b_{ki}a_{ik} = \sum_{k=1}^{n}(BA)_{kk} = \operatorname{tr}(BA).$$

□

Exercise 2. *Define the matrices R and S by* (4.12) *and* (4.13)*. Prove that $S = R^{-1}$.*

Proof. Treating the basis elements as column vectors, let $B = (v_1, \ldots, v_n)$ and $B' = (v_1', \ldots, v_n')$ be $n \times n$ matrices corresponding to the bases B and B'. By (4.12) and (4.13),

$$B' = RB \qquad \text{and} \qquad B = SB',$$

from which we obtain $B = SRB$. The columns of the matrix B, being the basis elements themselves, are linearly independent and thus B is invertible. Multiplying both sides by B^{-1}, we obtain $I = SR$, where I is the identity matrix of order n. It follows that $S = R^{-1}$. □

4.6 Gauss Sums and Quadratic Reciprocity

Exercise 1. *Show that*

$$\tau(5) = 2\left(\cos\frac{\pi}{5} + \cos\frac{2\pi}{5}\right).$$

Proof. By the definition of the classical Gauss sum,

$$
\begin{aligned}
\tau(5) &= \sum_{k=1}^{4}\left(\frac{k}{5}\right)e^{2\pi ik/5} \\
&= \left(\frac{1}{5}\right)e^{2\pi i/5} + \left(\frac{2}{5}\right)e^{4\pi i/5} + \left(\frac{3}{5}\right)e^{6\pi i/5} + \left(\frac{4}{5}\right)e^{8\pi i/5} \\
&= 2\left(\cos\frac{\pi}{5} + \cos\frac{2\pi}{5}\right).
\end{aligned}
$$

□

Exercise 2 is solved similarly.

Exercise 3. *Let p be an odd prime and χ_0 the principal character modulo p. Prove that if p divides a, then $\tau(a, \chi_0) = p - 1$.*

Proof. Since p divides a, we obtain $e^{2\pi iak/p} = 1$ for all $k \in \mathbb{Z}$. Then

$$\tau(\chi_0, a) = \widehat{\chi_0}(\psi_{-a}) = \sum_{k=0}^{p-1} \chi_0(k + p\mathbb{Z}) e^{2\pi iak/p} = \sum_{k=1}^{p-1} 1 = p - 1,$$

where we have used $\chi_0(p\mathbb{Z}) = 0$ and $\chi_0(k + p\mathbb{Z}) = 1$ when $\gcd(k, p) = 1$. □

Exercise 4. *Let*

4.7 The Sign of the Gauss Sum

5 The *abc* Conjecture

5.1 Ideals and Radicals