Elementary Number Theory

Robin Truax

January 2023

Contents

1 Introduction

One can summarize number theory as the study of the integers. Number theory incorporates ideas from many different areas of math, and is notorious for inspiring difficult proofs of results with simple statements. These notes will rely on ring-theoretic language, so it is helpful to have taken a first algebra course. Though we will define most of the ring-theoretic language we use, basic facts about groups will not be proven here (instead, check out my notes on Group Theory).

These notes draw on many sources, crudely cited where they are used, but roughly this is a summary of what I learned in Math 152 at Stanford and Baker's *A Comprehensive Course on Number Theory.*

2 Divisibility and Congruences in $\mathbb{Z}$

First, let's discuss the basic structure of the integers, especially with regards to prime factorization.

2.1 Rings and Integers

Definition 1 (Abelian Group)**.** An *abelian group* $(G, +)$ (denoted by G by abuse of notation) is a set G equipped with an binary operation $+$ such that:

1. There exists an element $0 \in G$ such that $a + 0 = 0 + a = a$ for all $a \in G$.
2. For any element $a \in G$, there exists $-a \in G$ such that $a + (-a) = 0 \in G$.
3. For any elements $a, b, c \in G$, $(a + b) + c = a + (b + c)$ (associativity) and $a + b = b + a$ (commutativity).

For example, the integers $\mathbb{Z}$ form an abelian group under the usual definition of addition.

Definition 2 (Ring)**.** A *ring* $(R, +, \cdot)$ (denoted by R by abuse of notation) is an abelian group $(R, +)$ equipped with an additional operation $\cdot$ satisfying the following axioms:

1. There exists an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$.
2. Given any elements $r, s, t \in R$, $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ (assocativity).
3. Given any elements a, b, c, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributivity).

All of our rings are furthermore *commutative*, so $a \cdot b = b \cdot a$.

For example, the integers $\mathbb{Z}$ form a ring under the usual definitions of addition and multiplication.

Definition 3 (Homomorphism)**.** Given two rings R and S, a function $\phi : R \to S$ is called a *ring homomorphism* if $\phi(r + r') = \phi(r) + \phi(r')$ and $\phi(rr') = \phi(r)\phi(r')$ for all $r, r' \in R$, and furthermore if $\phi(1) = 1$.

Definition 4 (Isomorphism)**.** A homomorphism $\phi : R \to S$ is called an *isomorphism of rings* if there exists a homomorphism $\psi : S \to R$ such that $\phi \circ \psi = \mathrm{id}_S$ and $\psi \circ \phi = \mathrm{id}_R$. Equivalently, an isomorphism is a bijective homomorphism.

Definition 5 (Image)**.** Given a homomorphism of rings $\phi : R \to S$, *the image of* ϕ is the set

$$\mathrm{im}\, \phi = \{\phi(r) \mid r \in R\} \subseteq S.$$

Definition 6 (Integral Domain)**.** A ring R is called an *integral domain* if $ab = 0$ implies that $a = 0$ or $b = 0$. Notice that if R is an integral domain, then $ac = bc$ implies that either $a = b$ or $c = 0$.

For example, the ring of integers is an integral domain.

Definition 7 (Unit)**.** An element $u \in R$ is a *unit* of R if there exists $v \in R$ such that $uv = vu = 1$. The set of all units of a commutative ring R forms an abelian group, denoted $R^\times$.

For example, the set of units in $\mathbb{Z}$ is simply $\{-1, 1\}$. This forms a group isomorphic to C_2.

Definition 8 (Field)**.** In any nonzero ring R, 0 cannot be a unit, since for any $r \in R$,

$$0 \cdot r = (0 + 0) \cdot r = 0 \cdot r + 0 \cdot r \Rightarrow 0 = 0 \cdot r.$$

However, if every *nonzero element* is a unit, then the ring R is called a *field*. Notice that any field is an integral domain, but not every integral domain is a field.

Definition 9 (Divides)**.** Given elements $a, b \in R$, we say that a *divides* b (and write $a \mid b$) if there exists $c \in R$ such that $ac = b$.

Definition 10 (Prime)**.** An element $p \in R$ is called *prime* if $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Definition 11 (Irreducible)**.** An element $i \in R$ is called *reducible* if there exist non-units $j, k \in R$ such that $i = jk$. An element which is not reducible is called *irreducible*.

In fact, with some investigation, one might discover that, in the integers, the prime elements and the irreducible elements are the same. Indeed, we will prove that $\mathbb{Z}$ is a unique factorization domain (UFD), which implies that the prime and irreducible elements are the same. However, unfortunately, this is not true in general. Let's take a look at an example.

Proposition 1. *Not all irreducible elements are prime in the ring* $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

Proof. Notice that $2 \cdot 3 = 6$, so 2 divides 6. To see why 2 is irreducible, consider a map which describes the "size" of an element in $\mathbb{Z}[\sqrt{-5}]$, called the *norm map*:

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

It is not difficult to check via computation that $N(\alpha\beta) = N(\alpha)N(\beta)$ for any $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Therefore, if $\alpha\beta = 2$, then $N(\alpha)N(\beta) = N(\alpha\beta) = N(2) = 4$. Either $N(\alpha)$ and $N(\beta)$ are both 2, or one of $N(\alpha)$ and $N(\beta)$ is 1, and the other is 4. Yet it is not difficult to check, from the formula, that there are no elements of norm 2. Therefore one of $N(\alpha)$ and $N(\beta)$ is 1. Yet the only elements with norm 1 are 1 and -1, which are both plainly units. Therefore, 2 cannot be written as the product of two non-units, so it is irreducible.

On the other hand, 6 is equal to $(1 + \sqrt{-5})(1 - \sqrt{-5})$. If 2 were prime, then it would divide at least one of these two elements. Yet it does not divide either, so it isn't prime. Thus, 2 is irreducible and not prime. □

Notice that the reason why this failed had something to do with the fact that we could write 6 as the product of irreducible elements in two different ways. Yet in $\mathbb{Z}$, each number can be uniquely expressed as the product of primes; we call this unique factorization, and it obstructs the separation of irreducible and prime elements.

2.2 Ideals

Definition 12 (Ideal)**.** An *ideal* I of a ring R is a subgroup of the abelian group $(R, +)$ which is also closed under scaling by R; that is, if $i \in I$ and $r \in R$, then $ri \in I$.

For example, the set of multiples of 2 is an ideal of $\mathbb{Z}$.

Definition 13 (Generated Ideals)**.** The ideal (S) *generated* by a set $S \subseteq R$ is the smallest ideal containing S; explicitly, it can be described as that is, (S) is the set of all finite R-linear combinations of elements in S

$$(S) = \left\{ \sum_{i=1}^{n} r_i s_i \;\middle|\; n \in \mathbb{Z}, r_i \in R, s_i \in S \right\}.$$

If S is a finite set $\{a_1, \ldots, a_n\}$, we abuse notation and abbreviate $(\{a_1, \ldots, a_n\})$ by $(a_1, \ldots, a_n)$.

Note: When we say that (S) is the "smallest ideal containing S", we are not making a statement about cardinality (often (S) has the same infinite cardinality as many other ideals containing S), but we mean that every ideal containing S must contain (S). In other words, (S) is minimal under the preorder of inclusion.

Definition 14 (Sum and Product of Ideals)**.** Suppose I and J are ideals of R. Then

$$I + J = \left\{ \sum_{k=1}^{n} i_k j_k \;\middle|\; n \in \mathbb{N}, i_k \in I, j_k \in J \right\} \qquad IJ = \left\{ ij \;\middle|\; i \in I, j \in J \right\}$$

Notice that $I + J = (I \cup J)$ is the smallest ideal containing I and J.

Definition 15 (Maximal)**.** An ideal I of R is called *maximal* if $I \subsetneq R$ and $J \supsetneq I$ implies $J = R$.

Definition 16 (Prime)**.** An ideal I of R is called *prime* if $ab \in I$ implies $a \in I$ and $b \in I$.

Proposition 2. *Any maximal ideal is prime.*

Proof. Suppose that $\mathfrak{m}$ is maximal and $ab \in \mathfrak{m}$. Then since $\mathfrak{m}$ is maximal and $(a, \mathfrak{m}) \supseteq \mathfrak{m}$, either $(a, \mathfrak{m}) = R$ or $(a, \mathfrak{m}) = \mathfrak{m}$. In the former case, $b \in a^{-1}\mathfrak{m} = \mathfrak{m}$, and in the latter case $a \in \mathfrak{m}$, so either way one of a or b is contained in $\mathfrak{m}$. Hence $\mathfrak{m}$ is prime. □

Definition 17 (Associates)**.** Two elements $a, b \in R$ are said to be *associates* if there exists a unit u such that $au = b$. Notice that this definition is symmetric; if $au = b$, then $a = bu^{-1}$. Associated elements are considered "the same" in many senses; in particular, if R is an integral domain, $(a) = (b)$ if and only if a and b are associates. Also, a divides b and b divides a if and only if a and b are associates.

In the ring of integers $\mathbb{Z}$, two elements are conjugate if and only if they differ by a sign.

2.3 UFDs, PIDs, and Euclidean Domains

In this section, we will review three important conditions on the structure of rings.

Definition 18 (UFD)**.** An integral domain R is called a unique factorization domain (UFD) if any $r \in R$ can be expressed as $up_1 \cdots p_n$ for some unit u and irreducible elements $p_1, \ldots, p_n$, in a unique way. In other words, in a UFD, if $r = up_1 \cdots p_n = vq_1 \cdots q_m$ (where u, v are units and both the p_i and q_i are irreducible), then $n = m$ and there exists a reordering of the q_i such that p_i and q_i are associated for each i.

By grouping together associated primes, we can write any element $r \in R$ uniquely in the form

$$up_1^{e_1} \cdots p_n^{e_n}$$

where the p_i are pairwise non-associated. This is often referred to as the *prime factorization* of r (even though the factorization above is also technically a factorization of r into primes).

You might notice that I say "prime factorization" instead of "irreducible factorization". This is no issue, as the following result shows:

Proposition 3. *In a UFD, prime and irreducible elements are the same.*

Proof. In fact, in an integral domain any prime is irreducible. Proving that any irreducible element i is prime amounts to taking the prime factorization of ab and noting that by unique factorization i must be conjugate to one of the factors in a (hence it divides a) or one of the factors in b (hence it divides b). □

Definition 19 (PID)**.** An integral domain R is called a *principal ideal domain* (PID) if every ideal I of R is *principal*; that is, of the form (r) for some $r \in R$.

It is not difficult to show that primes and irreducibles are the same in PIDs as well, via the following argument:

Proposition 4. *In a PID, any irreducible element i generates a maximal ideal and hence a prime ideal. Since (p) is prime if and only if p is a prime element, this implies that i is a prime element.*

Definition 20 (Euclidean Domain)**.** Suppose R is an integral domain. Then a function $N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ is called *Euclidean* if for any $a, b \in R$ with b nonzero, there exist $q, r \in R$ such that

$$a = bq + r$$

and either $N(r) < N(b)$ or $r = 0$. If R is a ring and there exists a Euclidean function on R, then we call R a *Euclidean domain*.

Theorem 5. *All Euclidean domains are PIDs.*

Proof. Suppose I is an ideal of a Euclidean domain R with Euclidean function N. Then let $b \in I$ be such that $N(b)$ is minimal among all nonzero elements of I. I claim that $I = (b)$. To see why, we will prove that $(b) \subseteq I$ and $I \subseteq (b)$. The first of these is easy: since $b \in I$, $(b) \subseteq I$.

On the other hand, suppose $a \in I$. Then by the properties of Euclidean functions we may write $a = bq + r$ for some q, r with $r = 0$ or $N(r) < N(b)$. But $r = a - bq \in I$, and b has minimal norm among all elements of I, so the latter case is impossible. Hence $r = 0$. Therefore $a = bq \in (b)$, so indeed $I \subseteq (b)$. □

Theorem 6. *All PIDs are UFDs.*

Proof. Let R be a principal ideal domain, and consider $r \in R$. First, we will show that r can be factored into a product of irreducibles. Suppose, for the sake of contradiction, that r cannot be factored into a product of irreducibles. Then clearly r cannot be irreducible itself, so $r = r_1 r_1'$ for some nonunits r_1, r_1'. But then at least one of r_1 and r_1' cannot be factored into a product of irreducibles (since otherwise we could multiply the factorizations) – assume without loss of generality that it is r_1.

Again, r_1 cannot be irreducible, so $r_1 = r_2 r_2'$ for some nonunits r_2, r_2' where (without loss of generality) r_2 cannot be factored into a product of irreducibles. We can repeat this process to get a sequence

$$r_1, r_2, \ldots$$

of elements of R such that $r_{i+1} \mid r_i$ and r_i and r_{i+1} are not associates for every i. Then we have a strictly ascending chain of ideals

$$(r_1) \subsetneq (r_2) \subsetneq \cdots$$

which I claim is impossible. To see why, verify that $\bigcup_{i=1}^{\infty}(r_i)$ is an ideal, and thus is generated by $r' \in R$. But by the definition of a union, $r' \in (r_n)$ for some n. But then $(r_n) \supseteq (r') = \bigcup_{i=1}^{\infty}(r_i) \supseteq (r_{n+1})$, which is impossible in a strictly ascending chain $(r_{n+1}) \supsetneq (r_n)$. Hence our assumption that r cannot be factored was incorrect, and we know that factorizations exist in a PID.

Hence it suffices to show that factorizations in a PID are unique. For this, we will use the fact that any irreducible element of a PID is prime, proven earlier. Now, suppose we have two factorizations, as so:

$$r = up_1 \cdots p_r = vq_1 \cdots q_s.$$

Since p_1 divides $q_1 \cdots q_s$, and it is prime since it is irreducible, p_1 divides q_i for some i. But q_i is irreducible, so p_1 can only divide q_i if p_1 and q_i are associates. Hence by adjusting units, we can cancel p_1 and q_i to get two factorizations with strictly fewer terms, and by repeating this process we may pair up associate p_i and q_j until there are none left, as desired. □

Proposition 7. *The ring of integers $\mathbb{Z}$ is a Euclidean domain.*

Proof. The function $N : \mathbb{Z} \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ given by $N(r) = |r|$ is Euclidean by the division algorithm. □

Corollary 7.1. *The ring of integers is a principal ideal domain and a unique factorization domain.*

Definition 21 (Greatest Common Divisor)**.** Since $\mathbb{Z}$ is a PID, given any set of integers S, the ideal (S) is principal with generator d. This d is unique up to sign, and is called the *greatest common divisor* of S, since it divides all the elements of S and any integer dividing all the elements of S divides d. We denote d by $\gcd(S)$. Abusing notation, we also write (a, b) for the greatest common divisor of a and b. Also, if $(a, b) = 1$, we say a and b are *coprime*.

2.4 Modular Arithmetic

Definition 22 (Equivalence Relation)**.** An *equivalence relation* $\sim$ on a set S is a binary relation satisfying

1. $a \sim a$ for any $a \in S$ (reflexivity)
2. $a \sim b$ implies $b \sim a$ for any $a, b \in S$ (symmetry)
3. $a \sim b$ and $b \sim c$ implies $b \sim c$ for any $a, b, c \in S$ (transitivity)

For example, given a family $\mathscr{F}$ of sets, we might say that $S \sim T$ iff there exists a bijection from S to T. This gives an equivalence relation (the equivalence relation of *cardinality*) on $\mathscr{F}$.

Definition 23 (Equivalence Class)**.** Given a set S with equivalence relation $\sim$, the *equivalence class* of s is

$$[s] = \{t \in S \mid s \sim t\}.$$

Notice that $t \in [s] \Leftrightarrow [t] = [s]$, and hence the set of all equivalence classes forms a partition of S.

Proposition 8. *Partitions on S and equivalence relations on S are in one-to-one correspondence as follows:*

1. *A partition $\{S_\lambda\}_{\lambda \in \Lambda}$ of S induces the equivalence relation $s \sim t$ iff $s, t \in S_\lambda$ for some $\lambda \in \Lambda$.*
2. *An equivalence relation $\sim$ on S induces a partition by considering the equivalence classes of $\sim$.*

Definition 24 (Quotient Ring)**.** If R is a ring with ideal I, *the quotient* R/I is the ring formed as follows:

1. Define an equivalence relation $\sim$ on R by $r \sim s$ iff $r - s \in I$.
2. Let the elements of R/I be the equivalence classes of R under $\sim$.
3. Define addition on R by $[a] + [b] = [a + b]$.
4. Define multiplication on R by $[a][b] = [ab]$.

One can verify that the notions of addition and multiplication are well-defined, and furthermore it is easy to check that R/I satisfies the ring axioms. Hence R/I is indeed a ring, called a *quotient ring*.

Definition 25 (Kernel)**.** The *kernel of a ring homomorphism* $\phi : R \to S$ is the set

$$\ker \phi = \{r \in R \mid \phi(r) = 0\}.$$

It is not difficult to verify that this is an ideal.

For example, the natural homomorphism $\pi : R \to R/I$ given by $r \mapsto [r]$ has kernel I.

Proposition 9. *A ring homomorphism $\phi : R \to S$ is injective iff* $\ker \phi = \{0\}$.

Proof. Necessarily, $\phi(0) = 0$. If $\phi : R \to S$ is injective, then the only element of R which can map to 0 is 0, so necessarily $\ker \phi = \{0\}$ in this case. On the other hand, suppose $\phi : R \to S$ is not injective. Then there exist distinct elements r_1 and r_2 such that $\phi(r_1) = \phi(r_2)$. But then $\phi(r_1 - r - 2) = \phi(r_1) - \phi(r_2) = 0$, so $r_1 - r_2$ is a nonzero element of $\ker \phi$ (whence $\ker \phi \neq \{0\}$). □

Definition 26 (Ring of Integers mod n)**.** The *ring of integers mod n* is the quotient ring $\mathbb{Z}/n\mathbb{Z}$, where $n\mathbb{Z} = (n) = \{nk \mid k \in \mathbb{Z}\}$. The elements of $\mathbb{Z}/n\mathbb{Z}$ are simply the equivalence classes $[0], [1], [2], \ldots, [n-1]$, called the *residue classes mod n*. Often by abuse of notation we drop the brackets.

Definition 27 (Equivalent Modulo n)**.** Two integers a and b are said to be *equivalent modulo n* if $[a] = [b] \in \mathbb{Z}/n\mathbb{Z}$. In this case we write $a \equiv b \bmod n$.

Modular arithmetic is often helpful for finding solutions to equations, or proving that no solutions exist. For example, consider the number 23487203. Can it be written as the sum of two perfect squares?

Even without using a computer, the answer is clearly "no". To see why, notice that if there exist x and y such that $x^2 + y^2 = 23487203$, then reducing modulo 4 we have

$$x^2 + y^2 \equiv 23487203 \equiv 3 \bmod 4.$$

But it is easy to check that $0^2 \equiv 0 \bmod 4$, $1^2 \equiv 1 \bmod 4$, $2^2 \equiv 0 \bmod 4$, and $3^2 \equiv 1 \bmod 4$. Hence the only possible values for sums of squares mod 4 are $0+0 \equiv 0 \bmod 4$, $0+1 \equiv 1 \bmod 4$, or $1+1 \equiv 2 \bmod 4 - 3 \bmod 4$ is not the sum of two squares. Hence 23487203 is not the sum of two squares.

We will solve this problem of the sums of two squares more generally later, but for now we emphasize that

1. because any equation in the integers can be reduced to an equation mod n,
2. any solution with integers becomes a solution mod n,
3. and mod n there are only a finite number of options to check

it is useful to reduce mod n to show that equations in the integers have no solution. However, not all problems can be solved this way; certain elliptic curves, for example, have no solutions in the integers but solutions in $\mathbb{Z}/n\mathbb{Z}$ for every n.

Theorem 10. *A residue class $[x] = x \bmod n$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if $(x, n) = 1$. In this case, $x \bmod n$ is called a reduced residue class mod n.*

Proof. Suppose $(x, n) = 1$. This implies $(x, n) = (1)$ as ideals, so in particular there exist $a, b \in \mathbb{Z}$ such that

$$ax + bn = 1 \Rightarrow ax - 1 = -bn \Rightarrow ax \equiv 1 \bmod n.$$

Hence in this case $[a]$ and $[x]$ are inverses in $\mathbb{Z}/n\mathbb{Z}$. On the other hand, suppose a is an inverse for $x \bmod n$. Then for some $b \in \mathbb{Z}$, $ax - 1 = bn$. Yet then $ax - bn = 1$, whence $1 \in (x, n)$. Since (1), the smallest ideal containing 1, is the entire ring, this forces $(x, n) = (1)$. Hence $(x, n) = 1$. □

Corollary 10.1. *The ring of integers mod n forms a field if and only if n is prime.*

Proof. This is because $1, \ldots, n-1$ are all coprime to n if and only if n is prime. □

Theorem 11 (Wilson's Theorem)**.** *$(n-1)! \equiv -1 \bmod n$ if and only if n is prime.*

Proof. If n is not prime, then plainly $(n-1)! \equiv 0 \bmod n$. Therefore assume n is prime. Then by Corollary 10.1, every nonzero residue class has an inverse, so in the factorial $(n-1)!$, nonzero residue classes will cancel out with their inverse – unless they are their own inverse. Hence

$$(n-1)! \equiv \prod_{\substack{x \bmod n \\ x^2 \equiv 1 \bmod n}} x \bmod n.$$

Yet $x^2 \equiv 1 \bmod n \Rightarrow x^2 - 1 \equiv 0 \bmod n \Rightarrow (x+1)(x-1) \equiv 0 \bmod n$, and since n is prime, we must either have $x + 1 = 0$ or $x - 1 = 0$. This implies that either $x = -1$ or $x = 1$, so

$$(n-1)! \equiv \prod_{\substack{x \bmod n \\ x^2 \equiv 1 \bmod n}} x \equiv -1 \cdot 1 \equiv -1 \bmod n.$$

□

2.5 The Infinitude of Primes

Theorem 12 (Euclid)**.** *There are infinitely many primes in* $\mathbb{Z}$*.*

Proof. Suppose, to the contrary, that there are finitely many primes $p_1, \ldots, p_n$ in $\mathbb{Z}$. Then consider

$$k = p_1 \cdots p_n + 1.$$

By unique factorization, k is divisible by a prime p. But $k \equiv 1 \bmod p_i$ for each i, so k is not divisible by any of the primes $p_1, \ldots, p_n$. Hence k is divisible by a prime not among $p_1, \ldots, p_n$, which is a contradiction. □

Proposition 13. *There are infinitely many primes of the form* $4k + 3$ *(where* k *is an integer).*

Proof. Suppose that there are finitely many primes $p_1, \ldots, p_n$ of the form $4k + 3$. Then consider

$$j = 4p_1 \cdots p_n - 1.$$

Now, j is odd, so it is the product of odd primes. Yet j cannot be solely the product of primes of the form $1 \bmod 4$, since then we would have $j \equiv 1 \bmod 4$, which is not true (indeed $j \equiv 3 \bmod 4$). Furthermore, j is not divisible by any of the primes $p_1, \ldots, p_n$, since $j \equiv -1 \bmod p_i$ for each i. Hence we may conclude that j is divisible by a prime of the form $4k + 3$ not among $p_1, \ldots, p_n$, the desired contradiction. □

It turns out the following fact is true, but you cannot prove it with the same method as Prop. 13. Why?

Proposition 14. *There are infinitely many primes of the form* $4k + 1$ *(where* k *is an integer).*

3 Arithmetical Functions

The formal definition of an arithmetical function is quite loose:

Definition 28 (Arithmetical Function)**.** An *arithmetical function* is a function $f : \mathbb{Z}^+ \to \mathbb{C}$.

However, the spirit of arithmetical functions is to investigate number-theoretic properties of the integers. The goal of the definition is simply to provide an umbrella term for these important functions.

3.1 Multiplicativity and Dirichlet Convolution

Definition 29 (Multiplicative)**.** An arithmetical function f is said to be *multiplicative* if whenever m and n are coprime, $f(mn) = f(m)f(n)$. Furthermore, f is said to be *totally multiplicative* if $f(mn) = f(m)f(n)$ for all positive integers m and n (not just pairwise coprime positive integers).

Definition 30 (Dirichlet Convolution)**.** Given two arithmetical functions f and g, their *Dirichlet convolution* is defined to be the arithmetical function given by

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

where the sum is ranging over all the positive integers d dividing n (called the *divisors* of n).

The reason why Dirichlet convolution is a powerful tool is the following fact:

Theorem 15. *If* f *and* g *are multiplicative arithmetical functions, then* $(f * g)$ *is also multiplicative.*

Proof. Suppose m and n are coprime, and consider the following:

$$(f * g)(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1d_2)g\left(\frac{m}{d_1} \cdot \frac{n}{d_2}\right) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2)g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right)$$

where, for the second equality, we notice that since m and n are coprime the divisors of mn can be split up into divisors of m and divisors of n, and for the third equality we are using the fact that f and g are multiplicative. Now, we will factor the final sum given, to see that

$$\sum_{\substack{d_1|m\\ d_2|n}} f(d_1)f(d_2)g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right) = \left(\sum_{d_1|m} f(d_1)g\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2|n} f(d_2)g\left(\frac{n}{d_2}\right)\right) = (f*g)(m)\cdot(f*g)(n),$$

which is the desired result. □

Theorem 16. *Dirichlet convolution is associative and commutative;* $(f*g)*h = f*(g*h)$ *and* $(f*g) = (g*f)$.

Proof. Not difficult, simply a matter of tedious computation. □

Following is an example application of Dirichlet convolution to proving that a function is multiplicative.

Definition 31 (σ-function)**.** The σ-function $\sigma(n)$ is defined to be the sum of all of the divisors of n, that is

$$\sigma(n) = \sum_{d|n} d.$$

Proposition 17. *The σ-function is multiplicative.*

Proof. Notice that if $\mathrm{id} : \mathbb{Z}^+ \to \mathbb{C}$ is the identity function $\mathrm{id}(n) = n$ and $1 : \mathbb{Z}^+$ is the trivial function $1(n) = 1$, then both id and 1 are totally multiplicative (and hence multiplicative) functions. But also

$$\sigma = (\mathrm{id} * 1)$$

so because the Dirichlet convolution of multiplicative functions is multiplicative, σ is multiplicative. □

3.2 The Chinese Remainder Theorem

Definition 32 (Direct Product)**.** Given two rings R and S, the *direct product of R and S*, denoted $R \times S$, is the ring on the underlying set $R \times S = \{(r, s) \mid r \in R, s \in S\}$ with operations given by

$$(r, s) + (r', s') = (r + r', s + s') \qquad (r, s)(r', s') = (rr', ss').$$

It is not difficult to generalize this notion to the direct product of n rings.

Theorem 18 (First Isomorphism Theorem)**.** *Suppose that $\phi : R \to S$ is a ring homomorphism. Then*

$$R/\ker\phi \simeq \operatorname{im}\phi.$$

Proof. Suppose that r_1 and r_2 are elements of R. Then $[r_1] = [r_2] \in R/\ker\phi$ if and only if $\phi(r_1) = \phi(r_2)$. To see why, notice that

$$[r_1] = [r_2] \Leftrightarrow r_1 - r_2 \in \ker\phi \Leftrightarrow \phi(r_1 - r_2) = 0 \Leftrightarrow \phi(r_1) - \phi(r_2) = 0 \Leftrightarrow \phi(r_1) = \phi(r_2).$$

In other words, there exists a well-defined and injective map $\iota : R/\ker\phi \to S$ given by $[r] \to \phi(r)$. It is easy to check that this map is a ring homomorphism. Furthermore, the image of ι is clearly $\operatorname{im}\phi$, so $\iota' : R/\ker\phi \to \operatorname{im}\phi$ is well-defined, injective, and surjective, so it is an isomorphism. □

Theorem 19 (The Chinese Remainder Theorem)**.** *Suppose that $n_1, \ldots, n_k$ are coprime integers. Then,*

$$\mathbb{Z}/(n_1 \cdots n_k)\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

along the isomorphism $x \bmod n_1 \cdots n_k \mapsto (x \bmod n_1, \ldots, x \bmod n_k)$.

Proof. Consider the map

$$\phi : \mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \text{ given by } x \mapsto (x \bmod n_1, \ldots, x \bmod n_k).$$

Since $n_1, \ldots, n_k$ are coprime, x is 0 mod n_i for each i if and only if x is 0 mod $n_1 \cdots n_k$. Therefore, $\ker \phi = (n_1 \cdots n_k)$. Hence the map

$$\overline{\phi} : \mathbb{Z}/(n_1 \cdots n_k)\mathbb{Z} \to \operatorname{im} \phi$$

given by $x \bmod n_1 \cdots n_k \mapsto (x \bmod n_1, \ldots, x \bmod n_k)$ is an isomorphism. Now, also notice that $\operatorname{im} \phi \subseteq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, yet because $\operatorname{im} \phi$ and $\mathbb{Z}/(n_1 \cdots n_k)\mathbb{Z}$ are isomorphic,

$$|\operatorname{im} \phi| = |\mathbb{Z}/(n_1 \cdots n_k)\mathbb{Z}| = n_1 \cdots n_k = |\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}|$$

and since $|\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}|$ is finite this implies that $\operatorname{im} \phi = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$. Hence $\overline{\phi} : \mathbb{Z}/(n_1 \cdots n_k)\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ given by $x \bmod n_1 \cdots n_k \mapsto (x \bmod n_1, \ldots, x \bmod n_k)$ is indeed an isomorphism, as desired. □

Corollary 19.1. *Suppose that the prime factorization of n is $p_1^{e_1} \cdots p_k^{e_k}$. Then*

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}.$$

In fact, a more general results exists, and though we will not prove it here, its statement is worth remembering.

Definition 33 (Coprime Ideals)**.** Two ideals I and J in a ring R are *coprime* if $I + J = R$.

Theorem 20 (The Chinese Remainder Theorems for Rings)**.** *Suppose that $I_1, \ldots, I_n$ are pairwise coprime ideals. Then $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$, and the natural map $R \to R/I_1 \times \cdots \times R/I_n$ is surjective with kernel $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$, so*

$$R/(I_1 \cdots I_n) \simeq R/(I_1 \cap \cdots \cap I_n) \simeq R/I_1 \times \cdots \times R/I_n.$$

3.3 The Euler φ-Function

Definition 34 (φ-function)**.** The φ-function is defined to be the arithmetical function

$$\phi(n) = |\mathbb{Z}/n\mathbb{Z}|^\times,$$

which by Theorem 10 is also equal to the number of elements of $\{1, \ldots, n-1\}$ coprime to n.

Proposition 21. *If p is prime, $\varphi(p) = p - 1$.*

Proof. Follows immediately from Corollary 10.1. □

Proposition 22. *If p is prime and $k \geq 1$, then $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$.*

Proof. Notice that the elements of $\{1, \ldots, p^k\}$ which are *not* coprime to p^k are the multiples of p; that is, $\{p, 2p, \ldots, p^{k-1}p\}$. There are p^{k-1} such elements, leaving $p^k - p^{k-1}$ elements of $\{1, \ldots, p^k\}$ coprime to p. □

Proposition 23. *φ is multiplicative.*

Proof. Suppose m and n are coprime. Then

$$\varphi(mn) = |(\mathbb{Z}/mn\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times|$$

where the second equality is the Chinese Remainder Theorem (Theorem 19). Yet notice that an element $(r, s) \in R \times S$ is a unit if and only if r is a unit of R and s is a unit of S. Hence,

$$\varphi(mn) = |(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(m)\varphi(n).$$

□

Corollary 23.1. *Suppose the prime factorization of n is $p_1^{e_1} \cdots p_k^{e_k}$. Then*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Proof. This follows immediately from Propositions 22 and 23. □

Theorem 24. $\sum_{d|n} \varphi(d) = n$.

Proof. Notice that $\sum_{d|n} \varphi(d)$ is equal to the Dirichlet convolution $\varphi * 1$, where $1 : n \to 1$ is the trivial arithmetical function. Since φ and 1 are both multiplicative, by Theorem 15 $\sum_{d|n} \varphi(d)$ is multiplicative. Hence it suffices to show that

$$\sum_{d|p^k} \varphi(d) = p^k$$

for every prime power p^k (since then by multiplicativity the result will follow). Yet this is simple:

$$\sum_{d|p^k} \varphi(d) = \varphi(1) + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^k) = 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) = p^k$$

with the final equality following by telescoping. □

Theorem 25 (Euler's Theorem)**.** *For any a and n with $(n, a) = 1$,*

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Proof. This is a consequence of Lagrange's Theorem (group theory) and the fact that $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group of order $\varphi(n)$. □

Corollary 25.1 (Fermat's Little Theorem)**.** *For any prime p and a not divisible by p,*

$$a^{p-1} \equiv 1 \bmod p.$$

Theorem 26. *$\phi(n)$ is even for all $n > 2$.*

Proof. Suppose that k is coprime to n. Then $n - k$ is coprime to n. Furthermore, if $n > 2$, then $k \neq n - k$ for all k coprime to n, since if $k = n - k$, then $k = \frac{n}{2}$ is not coprime to n. This implies that numbers $\{1, \ldots, n-1\}$ coprime to n come in pairs $\{k, n-k\}$ for all $n > 2$, whence $\phi(n)$ is even in this case. □

3.4 Möbius Inversion and Other Multiplicative Functions

Definition 35. For any positive integer n, the *Möbius function* is defined as follows:

$$\mu(n) = \begin{cases} 0 & p^2 \mid n \text{ for some prime } p, \\ (-1)^r & n = p_1 \cdots p_r \text{ for distinct primes } p_1, \ldots, p_r. \end{cases}$$

Since 1 is the empty product, $\mu(1) = (-1)^0 = 1$. Clearly, the Möbius function is multiplicative.

Theorem 27 (Möbius Inversion Formula)**.** *Suppose that f, g satisfy $g(n) = \sum_{d|n} f(d)$. Then,*

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Succintly, if $g = f * 1$ (where 1 is the constant function $n \mapsto 1$), then $f = \mu * g$.

Proof. Let ε be the arithmetical function defined by $\varepsilon(1) = 1$ and $\varepsilon(n) = 0$ for all $n > 1$. I claim that $\mu * 1 = \varepsilon$. To see why, first notice that clearly $(\mu * 1)(1) = \varepsilon(1) = 1$. Then, for any $n > 1$, write $n = p_1^{e_1} \cdots p_k^{e_k}$. Yet notice that $\mu(d)$ (for $d \mid n$) is only nonzero if d is the product of distinct primes among $p_1, \ldots, p_k$. Hence

$$\sum_{d|n} \mu(d) = \sum_{S \subseteq \{1,\ldots,k\}} \mu\left(\prod_{s \in S} p_s\right) = \sum_{S \subseteq \{1,\ldots,k\}} (-1)^{|S|} = \sum_{i=0}^{k} \binom{k}{i} (-1)^i = (1-1)^k = 0$$

where the third equality is grouping together terms corresponding to subsets of the same size and the fourth equality is simply the Binomial Theorem. Hence $(\mu * 1)(n) = \varepsilon(n)$ for any $n > 1$, so in general $\mu * 1 = \varepsilon$. Now, notice that $(f * \varepsilon) = (\varepsilon * f) = f$. Hence, by the associativity and commutativity of Dirichlet convolution (Theorem 16), we have that $\mu * g = g * \mu = (f * 1) * \mu = f * (1 * \mu) = f * (\mu * 1) = f * \varepsilon = f$. □

Definition 36. If f and g are arithmetical functions satisfying $g = f * 1$ and $f = \mu * g$, then f and g are said to be *Möbius transforms* of one another. In particular, f is multiplicative if and only if g is multiplicative (by the fact that the Dirichlet convolution of multiplicative functions is multiplicative, Theorem 15).

For example, the Euler φ-function and the identity map $n \mapsto n$ are Möbius transforms of one another. If we demonstrated this fact without relying on the multiplicativity of φ, it would provide an alternate proof of the fact that $var\phi$ is multiplicative.

4 Polynomials on $\mathbb{Z}/n\mathbb{Z}$

4.1 The Ring of Polynomials

Definition 37 (Ring of Polynomials)**.** Suppose that R is a ring. Then $R[X]$ is the ring of all polynomials of X with coefficients in R, with addition and multiplication defined as one would expect.

Definition 38 (Degree)**.** Let $f \in R[X]$ be a nonzero polynomial. Then f can be uniquely expressed as $a_n x^n + a_{n-1} x^n + \cdots + a_1 x + a_0$ for nonzero $a_n \in R$. We define n to be the degree of f, denoted $\deg(f)$.

Theorem 28 (Division Algorithm on Polynomials)**.** *Suppose that R is a ring. Then, for any polynomials $f, g \in R[X]$ such that the leading coefficient of g is a unit of R, there exist unique polynomials $q, r \in R[X]$ with $\deg r < \deg g$ and $f = qg + r$.*

Proof. This follows from polynomial long division, which works in any ring R as long as the leading coefficient of $g \in R[X]$ is a unit of R. □

Lemma 29. *If F is a field, then $F[X]$ is a Euclidean domain.*

Proof. By Theorem 28, $N(f) = \deg(f)$ is a Euclidean norm on $F[X]$. □

Lemma 30 (Correspondence Between Roots and Factors)**.** *Suppose R is an integral domain and f is a polynomial in $R[X]$. Then f has a root at a (i.e. $f(a) = 0$) if and only if $(X - a)$ is a factor of f.*

Proof. Suppose that $(X - a)$ is a factor of f. Then, by definition there is a polynomial g such that $f = g(X - a)$. But then $f(a) = g(a)(a - a) = 0$, as desired. On the other hand, suppose that $f(a) = 0$. Then, by the division algorithm, there exists $q, r \in R[X]$ such that $f = q(X - a) + r$ for some constant polynomial r. But then $f(a) = q(a - a) + r = r$, so $r = 0$. Hence $f = q(X - a)$, so $(X - a)$ is a factor of f. □

Definition 39 (Multiplicity of a Root)**.** Suppose that R is an integral domain and f is a polynomial in $R[X]$. Further suppose that a is a root of f. Then the *multiplicity of a* is the largest integer k such that $(X - a)^k$ divides f. We call a a *multiple root* of f if $k \geq 2$.

Definition 40 (Algebraic Derivative)**.** Let $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in R[X]$ be a polynomial. Then the *(algebraic) derivative of f(X)*, denoted f', is defined to be

$$a_n n X^{n-1} + a_{n-1}(n-1) X^{n-1} + \cdots + a_2 2X + a_1 \in R[X].$$

Notice that this derivative does *a priori* have anything to do with the ordinary derivative; this definition is made without any reference to the derivative of a real function. However, we will soon see that some key properties are shared, which is why this definition is still useful.

Lemma 31 (Properties of the Algebraic Derivative)**.** *Let R be an integral domain. Take f and g polynomials in $R[X]$ and $r, s \in R$ arbitrarily. Then,*

1. *$(rf + sg)' = rf' + sg'$ (the algebraic derivative is linear).*
2. *$(fg)' = fg' + f'g$ (the product rule for algebraic derivatives).*
3. *Suppose that $f(a) = 0$. Then a is a multiple root of f if and only if $f'(a) = 0$.*

Proof. Parts (1) and (2) amount to mechanical symbol manipulation, so we leave their proofs as an exercise to the reader. As for part (3), suppose that a is a multiple root of f. Then $f = (X-a)^2 g$ for some polynomial $g \in R[X]$. But then by part (2), $f' = (X-a)^2 g' + 2(X-a)g$, so indeed $f'(a) = 0$. On the other hand, suppose that a is not a multiple root of f. Then $f = (X-a)g$ for some polynomial $g \in R[X]$ with $g(a) \neq 0$. But then $f' = g + (X-a)g'$, so $f'(a) = g(a) + (a-a)g'(a) = g(a) \neq 0$, as desired. □

Theorem 32 (Taylor Series using the Algebraic Derivative)**.** *Just as Taylor series can be defined for real functions using the ordinary derivative can be applied to real polynomials, we may define the Taylor series of a polynomial $f(X) \in R[X]$ around $r \in R$ as follows:*

$$f(X) = \sum_{n=0}^{N} \frac{f^{(n)}(r)(X-r)^n}{n!}$$

where $N = \deg(f)$ and $f^{(n)}(r)$ is the nth derivative of f evaluated at r.

Proof. Since the derivative is linear by Lemma 31, it suffices to prove the result for a monomial. That is, without loss of generality we may assume $f(X) = X^N$. Next,

$$X^N = ((X-r)+r)^N = \sum_{n=0}^{N} \binom{N}{n} r^{N-n}(X-r)^n$$

Yet $\binom{N}{n} r^{N-n} = \frac{N(N-1)\cdots(N-n+1)r^{N-n}}{n!} = \frac{f^{(n)}(r)}{n!}$, so we have $X^N = \sum_{n=0}^{N} \frac{f^{(n)}(r)(X-r)^n}{n!}$, as desired. □

4.2 Hensel's Lemma

Hensel's Lemma is a powerful and surprising result about roots of polynomials modulo prime powers:

Lemma 33 (Hensel's Lemma)**.** *Let $f \in \mathbb{Z}[X]$. Also let $m \leq k$ be positive integers, and suppose $r \in \mathbb{Z}$ is such that*

$$f(r) \equiv 0 \bmod p^k \text{ and } f'(r) \not\equiv 0 \bmod p$$

then there exists an integer s (unique mod p^{k+m}) such that $f(s) \equiv 0 \bmod p^{k+m}$ and $r \equiv s \bmod p^k$.

Furthermore, suppose a is the multiplicative inverse of $f'(r)$ mod p^m (which exists because $(a,p) = 1$ implies $(a, p^m) = 1$). Then $s = r - f(r)a$.

Proof. Let s be an integer with $r \equiv s \bmod p^k$. Then $s - r = tp^k$ for some integer t. Now, by Theorem 32,

$$f(s) = \sum_{n=0}^{N} \frac{f^{(n)}(r)(tp^k)^n}{n!} = f(r) + tp^k f'(r) + \sum_{n=2}^{N} \frac{f^{(n)}(r)}{n!} t^n p^{kn}$$

Now, $f(r) \equiv 0 \bmod p^k$ implies $f(r) = zp^k$ for some integer z. Also define $g(t) = \sum_{n=2}^{N} \frac{f^{(n)}(r)}{n!} t^{n-2} p^{k(n-2)}$, so

$$f(s) = zp^k + tp^k f'(r) + p^{2k} t^2 g(t) = p^k(z + tf'(r)) + p^{2k} t^2 g(t).$$

Now, since $m \leq k$, $f(s) \equiv 0 \bmod p^{k+m}$ if and only if $p^k(z + tf'(r)) \equiv 0 \bmod p^{k+m}$, which happens if and only if $z + tf'(r) \equiv 0 \bmod p^m$. Now, let a be the multiplicative inverse of $f'(r) \bmod p^m$, which exists because $f'(r) \not\equiv 0 \bmod p$ implies that $f'(r)$ is coprime to p^m. Then we have $f(s) \equiv 0 \bmod p^{k+m}$ if and only if $t \equiv -za \bmod p^m$. Hence a unique solution for $t \bmod p^m$ exists, giving us a unique solution $s \bmod p^{k+m}$. □

Corollary 33.1. *Let $f \in \mathbb{Z}[X]$. Let k be a positive integer. Suppose $r \in \mathbb{Z}$ satisfies $f(r) \equiv 0 \bmod p$ and $f'(r) \not\equiv 0 \bmod p$. Then there exists an integer s such that $f(s) \equiv 0 \bmod p^k$.*

4.3 The Structure of $(\mathbb{Z}/n\mathbb{Z})^\times$

Recall from the Chinese Remainder Theorem (Theorem 19) and the reasoning of Proposition 23 that if $p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of n, then we can decompose the unit group of $\mathbb{Z}/n\mathbb{Z}$ as so:

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{e_k})^\times$$

Therefore, to understand the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$, it suffices to characterize the unit group of $(\mathbb{Z}/p^k\mathbb{Z})^\times$ for any prime power p^k. This is the focus of this section.

Definition 41 (Primitive Root)**.** A *primitive root mod n* is a reduced residue class $x \bmod n$ such that every reduced residue class mod n is a power of $x \bmod n$. In other words, $x \bmod n$ is a generator for the unit group $(\mathbb{Z}/n\mathbb{Z})^\times$ – it has order $\varphi(n)$. Plainly, such a generator exists if and only if the unit group is cyclic.

Proposition 34. *If there exists a primitive root mod n, there exist $\varphi(\varphi(n))$ primitive roots mod n.*

Proof. This follows from the group-theoretic fact that there exist $\varphi(k)$ generators of the cyclic group C_k. □

Theorem 35. *If p is a prime, the unit group $U = (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.*

Proof. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ has order $p - 1$, each element $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ has order dividing $p - 1$. Let d be the number of $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ with order d, so that necessarily $\sum_{d|(p-1)} \psi(d) = p - 1$.

Now, suppose that $\psi(d) \neq 0$. Then there exists $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ with order d. Then $1, a, \ldots, a^{d-1}$ are all distinct elements, and all of them satisfy the polynomial relation $X^d - 1 \equiv 0 \bmod p$. Yet it is well-known that in an integral domain, the number of roots of a polynomial cannot exceed its degree (since each root corresponds to a linear factor of the polynomial). Since $\mathbb{Z}/p\mathbb{Z}$ is a field, this implies that $X^d - 1 \equiv 0 \bmod p$ has at most d roots; yet $1, a, \ldots, a^{d-1}$ are d such roots.

Since any element of order d satisfies $X^d - 1 \equiv 0 \bmod p$, and the only roots of this polynomial are $1, a, \ldots, a^{d-1}$, all the elements of order d are contained in $1, a, \ldots, a^{d-1}$. Furthermore, it is not difficult to see that a^k has order d iff $(k, d) = 1$, whence $\psi(d) = \varphi(d)$ if $\psi(d) \neq 0$. Yet recall Theorem 24, which implies that $\sum_{d|(p-1)} \varphi(d) = p - 1$. Hence $\psi(d)$ must equal $\varphi(d)$ *everywhere*, since if $\psi(d) = 0$ for any d,

$$\sum_{d|(p-1)} \psi(d) < \sum_{d|(p-1)} \varphi(d) = p - 1$$

yet we know that the former is equal to the latter. Hence there exist $\varphi(p - 1) > 0$ elements of order $p - 1$, which implies that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, as desired. □

Theorem 36. *If p is an odd prime, the unit group $U = (\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic.*

Proof. We prove the following result: let g be a primitive root mod p, where p is an odd prime. Then for any fixed j, there exists an x such that $g' = g + px$ is a primitive root mod p^j. The proof is as follows.

Define $g' = g + px$. Now, $g^{p-1} = 1 + py$ for some integer y, so by the binomial theorem,

$$g'^{p-1} = 1 + pz, \text{ where } z \equiv y + (p - 1)g^{p-2}x \mod p.$$

Notice that because $(p-1)$ and g^{p-2} are relatively prime with p, we may choose x such that $(z,p)=1$. But then $g' = g + px$ is a primitive root mod p^j. To see this, suppose g' has order d mod p^j, so $d' \mid \phi(p^j) = p^{j-1}(p-1)$. Since g' is a primitive root mod p, $(p-1) \mid d$. Thus:

$$d = p^k(p-1) \text{ where } k < j \tag{1}$$

Since p is odd, we may use the binomial theorem to show that

$$g'^d = (g+px)^{(p-1)p^k} = (1+pz)^{p^k} = 1 + p^{k+1}z' \tag{2}$$

for some $(z', p) = 1$. Since $g'^d \equiv 1 \mod p^j$, we know that $j = k+1$, so $d = \phi(p^j)$, as desired. □

Theorem 37. *The unit group $U = (\mathbb{Z}/2^k\mathbb{Z})^\times$ is cyclic if $k = 1$ or 2 and isomorphic to the group $C_2 \times C_{2^{k-2}}$ otherwise (that is, if $k \geq 3$).*

Proof. 1 is a primitive root mod 2, and 3 is a primitive root mod 4.

Now, for the second part, we will begin with the following two lemmas:

Lemma 38. *For any positive integer $k \geq 2$, 5 mod 2^k has multiplicative order 2^{k-2}.*

Proof. To start, we show that for any k, $5^{2^k} = 1 + m2^{k+2}$ for some *odd* m. To prove this, we will use induction. For the base case, notice that for $k = 0$, $5^{2^0} = 5 = 1 + 1(2^{2+0})$, as desired. Now assume the result holds for k; that is, $5^{2^k} = 1 + m2^{k+2}$ for some odd m. Then,

$$5^{2^{k+1}} = \left(5^{2^k}\right)^2 = (1+m2^{k+2})^2 = 1 + m2^{k+3} + m^2 2^{2k+4} = 1 + (m + m^2 2^{k+1})2^{k+3}$$

and indeed $m + m^2 2^{k+1}$ is odd because clearly $m^2 2^{k+1}$ is even.

Yet this implies that the order of 5 mod 2^k is 2^{k-2} for $k \geq 2$. To see why, note that $5^{2^{k-2}} = 1 + m2^k$ implies $5^{2^{k-2}} \equiv 1 \mod 2^k$. On the other hand, as above, $5^{2^{k-3}} \equiv 1 + m2^{k-1} \equiv 1 + 2^{k-1} \not\equiv 1 \mod 2^k$. Thus, since the order of 5 divides 2^{k-2} but doesn't divide 2^{k-3}, we have that the order of 5 is 2^{k-2}, as desired. □

Lemma 39. *There does not exist any $n \in \mathbb{Z}$ for which $5^n \equiv -1 \mod 2^k$ for any $k \geq 2$.*

Proof. Since 5 has order 2^{k-2}, if any such n exists, we can find one in the set $\{1, \ldots, 2^{k-2}\}$. Thus, suppose that $n \in \{1, \ldots, 2^{k-2}\}$ is such that $5^n \equiv -1$. Then $5^{2n} \equiv 1$, which implies that 2^{k-2} divides $2k$. Since n lies in the set $\{1, \ldots, 2^{k-2}\}$, we must either have $n = 2^{k-2}$ or $n = 2^{k-3}$. Yet, in either case, $5^n \not\equiv -1$:

$$5^{2^{k-2}} \equiv 1 \mod 2^k \textbf{ and } 5^{2^{k-3}} \equiv 1 + 2^{k-1} \mod 2^k$$

This is a contradiction, so no such k exists. □

Corollary 39.1. *If $k \geq 2$, $5^m \not\equiv -5^n \mod 2^k$ for any integers m or n.*

Proof. Suppose that $5^m \equiv -5^n \mod 2^k$ for some positive integers m or n. Then $5^{m-n} \equiv -1 \mod 2^k$, a contradiction with the above result. □

Corollary 39.2. *If $k \geq 2$, every reduced residue class mod 2^k can be expressed as $\pm 5^n$ for a unique $n \in \{1, \ldots, 2^{k-2}\}$.*

Proof. There are $\phi(2^k) = 2^{k-1}$ reduced residue classes mod 2^k. At the same time, the elements of the form $\{5^n \mid n \in \{1, \ldots, 2^{k-2}\}\}$ and the elements of the form $\{-5^n \mid n \in \{1, \ldots, 2^{k-2}\}\}$ are each sets of 2^{k-2} distinct reduced residue classes mod 2^k, and they are distinct from each other by the above corollary. □

The unique expression of each reduced residue class in the form $\pm 5^n$ with $n \in \{1, \ldots, 2^{k-2}\}$ gives an isomorphism $\phi : (\mathbb{Z}/2^k\mathbb{Z})^\times \to C_2 \times C_{2^{k-2}}$. To see why, let -1 generate C_2 and c generate $C_{2^{k-2}}$. Then,

$$\phi(x) = \begin{cases} (1, c^n) & x \equiv 5^n \bmod 2^k \\ (-1, c^n) & x \equiv -5^n \bmod 2^k. \end{cases}$$

is not only a homomorphism, but is a bijection (and hence an isomorphism) by uniqueness. □

Theorem 40. *There exists a primitive root mod n if and only if n is 2, 4, p^k, $2p^k$ for an odd prime p.*

Proof. This proof is split into two parts:

Sufficiency: Theorem 35 and 37 prove that there exists a primitive root mod 2, 4, and p^k, so it suffices to find a primitive root mod $2p^k$. Yet notice that if p is an odd prime, $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$, any primitive root mod p^k, so it suffices to find a primitive root g of p^k which is coprime to $2p^k$. Indeed, it suffices for g to be odd, since it is already coprime to p^k. Yet for any such primitive root g, either g or $g + p^k$ is odd, so in either case we are done.

Necessity: Suppose n is a composite number which is not a power of a prime or twice the power of a prime. Then write $n = n_1 n_2$ where n_1, n_2 are both greater than 2 and coprime. Notice that $\varphi(n_1)$ and $\varphi(n_2)$ are both even, by Theorem 26. Now, for any natural number a,

$$a^{\frac{1}{2}\varphi(n)} \equiv \left(a^{\varphi(n_1)}\right)^{\frac{1}{2}\varphi(n_2)} \equiv 1 \bmod n_1 \qquad a^{\frac{1}{2}\varphi(n)} \equiv \left(a^{\varphi(n_2)}\right)^{\frac{1}{2}\varphi(n_1)} \equiv 1 \bmod n_2$$

whence the Chinese Remainder Theorem $a^{\frac{1}{2}\varphi(n)} \equiv 1 \bmod n$. Hence a is not a primitive root. The case of powers of two greater than 4 is handled by applying Theorem 37 and noticing that $C_2 \times C_{2^{k-2}} \ncong C_{2^{k-1}}$. □

5 Quadratic Residues

Definition 42 (Quadratic Residue)**.** Suppose x is an integer which is nonzero mod n. Then we say x is a *quadratic residue* mod n if there exists an integer y with $x \equiv y^2 \bmod n$, and a *quadratic nonresidue* otherwise.

Proposition 41. *For any odd prime p, there are exactly $\frac{p-1}{2}$ quadratic residues mod p. That is, half of all the nonzero residue classes mod p are quadratic residues.*

Proof. Suppose p is an odd prime. Then the map $\phi : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ given by $x \mapsto x^2$ is a homomorphism whose image is precisely the set of quadratic residues mod p. Now suppose $x \in \ker\phi$. Then

$$x^2 \equiv 1 \bmod p \Leftrightarrow x^2 - 1 \equiv 0 \bmod p \Leftrightarrow (x+1)(x-1) \equiv 0 \bmod p \Leftrightarrow x = \pm 1.$$

Hence $\ker\phi = \{-1, 1\}$ has cardinality 2. But the number of quadratic residues is equal to the size of $\operatorname{im}\phi$, which by the first isomorphism theorem is equal to $|(\mathbb{Z}/p\mathbb{Z})^\times / \ker\phi| = \frac{p-1}{2}$, as desired. □

5.1 The Legendre Symbol and Euler's Criterion

Definition 43 (Legendre Symbol)**.** Suppose $a \in \mathbb{Z}$ and p is prime. Then *the Legendre symbol of a* mod p is

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \bmod p \\ 1 & a \text{ is a quadratic residue mod } p \\ -1 & a \text{ is a quadratic nonresidue mod } p. \end{cases}$$

Proposition 42 (Euler's Criterion)**.** *If p is an odd prime and a is an integer, then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$$

Proof. If a is 0 mod p, the result follows trivially. Otherwise, notice that by Fermat's Little Theorem (Theorem 25.1), $a^{\frac{p-1}{2}}$ has square 1 mod p, so it is either equal to 1 or -1. Hence it suffices to show that $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ iff a is a quadratic residue mod p.

For this, let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and write $a \equiv g^k \bmod p$ for some minimal positive integer k. Notice that a is a quadratic residue mod p if and only if k is even. But k if even if and only if $a^{\frac{p-1}{2}} \equiv g^{k\frac{p-1}{2}}$ is equal to 1 mod p, so the desired result follows. □

Corollary 42.1. *The Legendre symbol is multiplicative; that is,* $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

Corollary 42.2. -1 *is a quadratic residue mod* p *if and only if* $p \not\equiv 3 \bmod 4$.

5.2 Gauss' Lemma and Zolotarev's Lemma

Definition 44 (Numerically Least Residue)**.** For any integer a and any natural number n we define the numerically least residue of a mod n as that integer a' such that $a \equiv a' \bmod n$ and $-\frac{n}{2} < a' \leq \frac{n}{2}$.

Lemma 43 (Gauss' Lemma)**.** *Let* p *be an odd prime and suppose that* a *is nonzero mod* p*. Furthermore, let* n *be the number of* $j \in \{1, \ldots, \frac{p-1}{2}\}$ *such that the numerically least residue of* $aj \bmod p$ *is negative. Then*

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Proof. Let $Z \equiv a \cdot 2a \cdots \frac{p-1}{2}a \bmod p$. On one hand, $Z \equiv a^{\frac{p-1}{2}}\left(1 \cdot 2 \cdots \frac{p-1}{2}\right)$. On the other hand, by replacing aj with its numerically least residue and factoring out the negative sign if necessary, we find that

$$Z \equiv (-1)^n \left(1 \cdot 2 \cdots \frac{p-1}{2}\right).$$

Hence $a^{\frac{p-1}{2}} \equiv (-1)^n$, and the result follows by Euler's criterion. □

Corollary 43.1. $\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}$*. In other words,* 2 *is a quadratic residue of all primes* $p \equiv \pm 1 \bmod 8$ *and a quadratic nonresidue of all primes* $p \pm 3 \bmod 8$.

Proof. If $a = 2$, the numerically least residue of aj is positive and equal to $2j$ for $1 \leq j \leq \left\lfloor \frac{p}{4} \right\rfloor$ and equal to $2j - p$ otherwise. Hence $n = \frac{1}{2}(p-1) - \left\lfloor \frac{p}{4} \right\rfloor$, which one can calculate is equivalent to $\frac{p^2-1}{8} \bmod 2$. □

Lemma 44 (Zolotarev's Lemma)**.** *Suppose that* p *is an odd prime and* $(a, p) = 1$*. Then*

$$\left(\frac{a}{p}\right) = \operatorname{sgn}(\pi_a)$$

where $\pi_a : x \mapsto ax$ *is a permutation on* $(\mathbb{Z}/p\mathbb{Z})^\times$*, so* $\operatorname{sgn}(\pi_a)$ *is the sign (or parity) of* π_a*.*

Proof. Consider the following table of all the numerically least residues coprime to p:

1	2	$\cdots$	$\frac{p-1}{2}$
-1	-2	$\cdots$	$\frac{p+1}{2}$

Then, apply the permutation $\pi_a : x \mapsto ax$ to get a rearranged table. Again, we will stick with the numerically least residues, so whenever ax is not a numerically least residue, replace it with its numerically least residue.

a	$2a$	$\cdots$	$\left(\frac{p-1}{2}\right)a$
$-a$	$-2a$	$\cdots$	$\left(\frac{p+1}{2}\right)a$

Now, apply another permutation ϕ to this table which swaps the two cells in a column if the top one is negative. Notice that the number of transpositions required for ϕ is precisely n (as it was defined in the statement of Gauss' Lemma, Lemma 43). Hence $\operatorname{sgn}(\phi) = (-1)^n$, which by Gauss' Lemma is equal to $\left(\frac{a}{p}\right)$.

I claim that ϕ and π_a have the same sign; this would suffice to prove the desired result. To prove this, notice that two permutations σ and τ on the same set have the same sign iff $\sigma\tau$ (or $\tau\sigma$) is even. Now, $\phi\pi_a$ does the exact same thing to the top row as it does to the bottom row; that is, $\phi\pi_a$ can be expressed as a permutation of only top row combined with the exact same permutation of the bottom row. Hence $\phi\pi_a$ must be the product of an even number of transpositions, so it is even, as desired. □

Following is another, more group-theoretic proof:

Proof. Consider the group homomorphism $f : (\mathbb{Z}/p\mathbb{Z})^\times \to \{-1, 1\}$ given by $f(a) = \operatorname{sgn}(\pi_a)$. Now, f is also surjective. To see why, first notice that $f(1) = 1$. Then let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Then $\operatorname{sgn}(\pi_g)$ is a $(p-1)$-cycle, which is composed of $p-2$ transpositions. This is an odd number of transpositions, so $f(g) = \operatorname{sgn}(\pi_g) = -1$, as desired.

Now, since f is surjective, by the First Isomorphism Theorem and counting, $\ker f$ must have index 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$. But $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, so it has a unique subgroup of any index, and the set of quadratic residues has index 2 by Proposition 41. Hence we are done. □

5.3 The Law of Quadratic Reciprocity

Next, we'll use Zolotarev's Lemma for an elegant proof of The Law of Quadratic Reciprocity, which is

Theorem 45 (The Law of Quadratic Reciprocity)**.** *If p and q are distinct odd primes, then*

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

In particular $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless $p \equiv q \equiv 3 \bmod 4$, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

To prove this result, we'll use the following lemma, derived from Zolotarev's Lemma:

Lemma 46. *Suppose p and q are odd primes, $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ and $b \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then define $\phi : x \mapsto b + qx$ and $\psi : x \mapsto a + px$. Then it follows that $\left(\frac{p}{q}\right) = \operatorname{sgn}(\phi)$ and $\left(\frac{q}{p}\right) = \operatorname{sgn}(\psi)$.*

Proof. Define $\sigma : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ by $\sigma(x) = a + x$. This permutation consists of a single q-cycle $(x, a+x, 2a+x, \ldots, (q-1)a+x)$. Therefore, σ is the product of $q-1$ transpositions, so $\operatorname{sgn}(\sigma) = 1$. Yet notice that $\phi = \sigma\pi_p$, so $\operatorname{sgn}(\phi) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\pi_p) = \operatorname{sgn}(\pi_p) = \left(\frac{p}{q}\right)$. The case $\operatorname{sgn}(\psi)$ follows identically. □

Now we can prove the Law of Quadratic Reciprocity.

Proof. Let p and q be distinct odd primes. Then, define $\iota : \mathbb{Z}/pq\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ to be the isomorphism given by the Chinese Remainder Theorem. Also define $\phi', \psi' : (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ by

$$\phi'(a, b) = (a, a + pb) \qquad \psi'(a, b) = (b + qa, b).$$

Define the permutation $\varphi : \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/pq\mathbb{Z}$ by $\varphi(a + pb) = qa + b$. Though it may not be obvious, by the Chinese Remainder Theorem this is well-defined.

Now, $\varphi = \iota^{-1} \circ \psi' \circ \phi'^{-1} \circ \iota$ and hence $\operatorname{sgn}(\varphi) = \operatorname{sgn}(\psi')\operatorname{sgn}(\phi'^{-1}) = \operatorname{sgn}(\psi')\operatorname{sgn}(\phi')$.

Now consider ϕ'. If we restrict this to $\{a\} \times (\mathbb{Z}/q\mathbb{Z})$ for any $a \in \mathbb{Z}/p\mathbb{Z}$, then ϕ' is simply the permutation ϕ defined in Lemma 46, which has sign $\left(\frac{p}{q}\right)$. But then ϕ' is the composition of p permutations with sign $\left(\frac{p}{q}\right)$, so ϕ' has sign $\left(\frac{p}{q}\right)^p = \left(\frac{p}{q}\right)$. Similar logic shows that $\operatorname{sgn}(\psi') = \left(\frac{q}{p}\right)$. Hence

$$\operatorname{sgn}(\varphi) = \operatorname{sgn}(\phi') \operatorname{sgn}(\psi') = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right).$$

On the other hand, we can compute the sign of φ directly. For this, recall that the sign of a permutation σ on a totally ordered set is equal to (and sometimes defined as) $(-1)^N$, where N is the number of inversions of σ (pairs (i, j) with $i < j$ and $\sigma(i) > \sigma(j)$). Counting these inversions is not difficult: it turns out that the requisite pairs are precisely those $(a_1 + pb_1, a_2 + pb_2)$ such that $a_1 > a_2$ and $b_2 > b_1$. Hence the pairs of distinct doubles $\{a_1 \bmod p, a_2 \bmod p\}$ and $\{b_1 \bmod q, b_2 \bmod q\}$ are in correspondence with the inversions. Hence there are $\frac{p(p-1)}{2} \cdot \frac{q(q-1)}{2} \equiv \frac{(p-1)(q-1)}{4} \bmod 2$ inversions of φ, so

$$(-1)^{\frac{(p-1)(q-1)}{4}} = \operatorname{sgn}(\varphi) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$$

as desired. □

6 Quadratic Forms

Definition 45 (Binary Quadratic Form)**.** A *binary quadratic form* is a polynomial of the form $f(x, y) = ax^2 + bxy + cy^2$ for integers a, b, c. The form is called *primitive* if $(a, b, c) = 1$.

Definition 46 (Discriminant)**.** The *discriminant* of a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is $d = b^2 - 4ac$. Notice that $d \equiv 0 \bmod 4$ if b is even and $d \equiv 1 \bmod 4$; this will be be relevant later.

Definition 47 (Representation)**.** An integer n is said to be *represented* by $f(x, y)$ if there exist a and b with $f(a, b) = n$, and n is *primitively represented* if furthermore $(a, b) = 1$.

6.1 Equivalent Quadratic Forms

Definition 48 (Equivalent Binary Quadratic Forms)**.** Two binary quadratic forms $f(x, y)$ and $g(x, y)$ are called *equivalent* if there exists an integer matrix

$$M = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$$

with determinant 1 and associated transformation $M : \mathbb{Z}^2 \to \mathbb{Z}^2$ such that $f \circ M = g$. Since M has determinant 1, M^{-1} is also an integer matrix with determinant 1 satisfying $f = g \circ M^{-1}$. Hence our notion of equivalence of binary quadratic forms is an equivalence relation.

Proposition 47. *Equivalent binary quadratic forms (primitively) represent the same integers and have the same discriminant.*

Proof. Suppose f and g are equivalent binary quadratic forms. Then $f \circ M = g$ for some 2×2 integer matrix with determinant 1. But then M^{-1} is also an integer matrix, and $f = g \circ M^{-1}$. Hence any (primitive) solution (a, b) to $f(x, y) = n$ can be made into a (primitive) solution $M^{-1}(a, b)$ for $g(x, y) = n$, and vice versa. Mechanical computation (substituting $x = px' + qy'$ and $y = qx' + sy'$ and simplifying) suffices to prove that binary quadratic forms have the same discriminant. □

Definition 49 (Principal Forms)**.** A binary quadratic form $f(x, y)$ is called a *principal form* if

1. $f(x, y) = x^2 - \frac{d}{4}y^2$ and $d \equiv 0 \bmod 4$.
2. $f(x, y) = x^2 + xy + \frac{1-d}{4}y^2$ and $d \equiv 1 \bmod 4$.

In either case, the principal form has discriminant d.

Proposition 48 (Output of Binary Quadratic Forms)**.** *Let $f(x,y) = ax^2 + bxy + cy^2$ be a binary quadratic form with discriminant d. If d is negative, then $f(x,y)$ is either always nonnegative (if a is positive) and we call it* positive definite *or always nonpositive (if a is negative) and we call it* negative definite*. Otherwise, we call $f(x,y)$* indefinite*, as it can be positive, negative, or zero.*

Proof. One can verify that $4af(x,y) = (2ax+by)^2 - dy^2$. From this alone the result follows; if $d \leq 0$ then $(2ax+by)^2 - dy^2$ is the sum of two squares and therefore only nonnegative. □

6.2 Reduced Quadratic Forms and Class Numbers

Assume, for this section, that f is a positive definite binary quadratic form. That is, $f(x,y) = ax^2+bxy+cy^2$ satisfies $d = b^2 - 4ac < 0$ and $a > 0$; accordingly, we must have $c > 0$.

Definition 50 (Reduced Binary Quadratic Forms)**.** Let $f(x,y) = ax^2 + bxy + cy^2$ be a positive definite binary quadratic form. Then f is called *reduced* if either of the following equalities hold

$$-a < b \leq a < c \text{ or } 0 \leq b \leq a = c.$$

Proposition 49. *Assume f is positive definite. Then f is equivalent to a reduced binary form.*

Proof. If $f(x,y) = ax^2 + bxy + cy^2$ is positive definite, i.e., $d < 0$ and $a > 0$. Notice that this implies that $c > 0$. Then I claim that a finite product of substitution matrices of the form

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

suffices to transform f into a positive definite form. To see why, notice that the first transformation swaps a and c, while leaving the absolute value of b unchanged. The second transformation has the effect of leaving a unchanged, changing b to $b+2a$, and increasing c. Similarly, the third transformation leaves a unchanged, changes b to $b-2a$, and increases c. It is clear from this description that the result follows. □

Lemma 50. *For any integer d, there are only finitely many reduced forms with discriminant d.*

Proof. By the inequalities defining reduced forms (and the fact that a and c are positive), we have $ac \geq b^2$. Hence $-d = 4ac - b^2 \geq 3ac$, implying that $|\frac{d}{3}| \geq a, c$. Hence there are only finitely many options for a and c, and since $|b|$ is bounded by a, we also have only finitely many options for b. □

Definition 51 (Class Number)**.** The *class number* $h(d)$ is the number of reduced binary quadratic forms with discriminant d.

Theorem 51. *$h(-4) = 1$; that is, the only reduced binary quadratic form with discriminant -4 is $x^2 + y^2$.*

Proof. Suppose that $f(x,y) = ax^2 + bxy + cy^2$ is reduced. Then $b^2 \leq ac$, so

$$b^2 - 4ac = -4 \Rightarrow 4 = 4ac - b^2 \Rightarrow 4 \geq 3ac \Rightarrow a = 1, c = 1$$

where the final equality follows because, as discussed earlier, $a > 0$ and $c > 0$. □

Lemma 52. *Any two distinct reduced quadratic forms are not equivalent.*

Proof. Suppose that $f(x,y) = ax^2 + bxy + cy^2$ is reduced. Now, if $x, y \in \mathbb{Z}$ are nonzero with $|x| \geq |y|$, then

$$\begin{aligned} f(x,y) &= ax^2 + bxy + cy^2 \geq a|x|^2 - |bxy| + c|y|^2 \geq a|x|^2 - |bx^2| + c|y|^2 \\ &= a|x|^2 - |b||x|^2 + c|y|^2 = |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c \end{aligned}$$

Similar logic shows that this bound also holds under the assumption $|y| \geq |x|$. Notice that this bound is tight, as one of $(x,y) = (1,1)$ or $(x,y) = (1,-1)$ achieves this bound. On the other hand, suppose we allow exactly one of x or y to be nonzero. Then the smallest values we can assume are at $(1,0)$ and $(0,1)$, which

result in a and c respectively. Therefore, the smallest values that $f(x,y)$ will take with x and y coprime are a, c, and $a-|b|+c$ in that order (order follows by the inequalities defining reduced forms).

Now let $g(x,y) = a'x^2 + b'xy + c'y^2$ be reduced and equivalent to $f(x,y)$. Our goal is to show that $f(x,y) = g(x,y)$. Yet we know the minimal values that $g(x,y)$ will take with x and y coprime are a', c', and $a' - |b'| + c'$ in that order. Since equivalent forms primitively represent the same integers (Prop. 47), this implies that $a = a'$ and $c = c'$. But then that implies that $|b| = |b'|$, so either $b = b'$ or $b = -b'$.

In the former case, we are immediately done. Therefore, assume $b = -b'$. Now, if $a = c$, then by the inequalities defining reduced forms, $0 \leq b \leq a = c$ and $0 \leq b' \leq a = c$, whence $b = b' = 0$ (by the relation $b = -b'$) and we're done. Therefore, we must have $a < c$, and in fact

$$-a < b \leq a < c \qquad -a < b' \leq a < c.$$

In fact, since $b = -b'$, we can refine the inequalities to $-a < b < a < c$ and $-a < b' < a < c$. This implies that $a - |b| + c > c > a$ for all nonzero integers x and y.

Since f and g are equivalent, there exists a unimodular matrix

$$M = \begin{bmatrix} p & q \\ r & s \end{bmatrix}.$$

such that its associated map under the standard basis, $M : \mathbb{Z}^2 \to \mathbb{Z}^2$, satisfies $f \circ M = g$. Now, in general, we have $f(p,r) = a'$ and $f(q,s) = c'$, but since $a = a'$ and $c = c'$, we have

$$a = ap^2 + bpr + cr^2 \Rightarrow p = \pm 1, r = 0 \qquad c = aq^2 + bqs + cs^2 \Rightarrow s = \pm 1, q = 0.$$

Notice we use that c is *strictly greater* than a for this result, which implies the only possible matrices are

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Yet all of these substitutions leave the b-coefficient unchanged, proving that $b = b' = 0$ in this case also. □

Corollary 52.1. *The class number $h(d)$ equals the number of nonequivalent positive definite binary quadratic forms with discriminant d.*

6.3 Representing Numbers with Quadratic Forms

Theorem 53. *n is primitively represented by some binary form with discriminant d if and only if there exists $m \in \mathbb{Z}$ such that $m^2 \equiv d \bmod 4n$.*

Proof. Suppose that $f(x,y) = ax^2 + bxy + cy^2$ primitively represents n; that is, p and r are coprime and satisfy $f(p,r) = n$. Since p and r are coprime, there exist q and s satisfying $ps - qr = 1$, so

$$M = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$$

is a unimodular matrix taking $f(x,y)$ to an equivalent form $g(x,y) = a'x^2 + b'xy + c'y^2$ satisfying $a' = n$. But f and g have the same discriminant, so $b'^2 - 4nc' = d$, so $m^2 \equiv d \bmod 4n$ has a solution $m = b'$.

On the other hand, suppose that m satisfies $m^2 \equiv d \bmod 4n$. Then there exists an integer c such that $m^2 - 4nc = d$. Yet then the binary quadratic form

$$nx^2 + mxy + cy^2$$

primitively represents n by $(x,y) = (1,0)$ and has determinant d by construction. □

6.4 Sums of Two and Four Squares

We will use the developed tools (in particular the fact that $h(-4) = 1$) to find which numbers are the sums of two squares.

Lemma 54. *A prime number p can be expressed as the sum of two squares iff $p \not\equiv 3 \bmod 4$.*

Proof. The only even prime is 2, which is equal to $1^2 + 1^2$. Now, if $p \equiv 3 \bmod 4$, then p cannot be the sum of two squares since the only quadratic residues mod 4 are 0 and 1, implying $x^2 + y^2$ is equivalent to 0, 1, or 2 mod 4. Hence, it suffices to prove that all primes $p \equiv 1 \bmod 4$ are the sum of two squares.

First, let $d = -4$. Then p is primitively represented by a binary quadratic form with discriminant d if there exists m satisfying $m^2 \equiv -4 \bmod 4p$. Yet -1 is a quadratic residue mod any prime $p \equiv 1 \bmod 4$ (see Corollary 42.2), so there exists m satisfying $m^2 \equiv -1 \bmod p$ and hence satisfying $m^2 \equiv -4 \bmod 4p$.

Therefore, p is primitively represented by a binary quadratic form $f(x, y)$ with discriminant -4. Since $f(x, y)$ has negative discriminant, it is definite, and since p is positive, $f(x, y)$ must be positive definite. But then, since $h(-4) = 1$, $f(x, y)$ is equivalent to the unique reduced form $x^2 + y^2$ of discriminant -4. Hence p is primitively represented by $x^2 + y^2$, as desired. □

Theorem 55 (Two Square Theorem)**.** *A natural number n can be expressed in the form $x^2 + y^2$ for some integers x, y if and only if every prime divisor p of n with $p \equiv 3 \mod 4$ occurs to an even power in the prime factorization of n.*

Proof. Suppose, for the sake of contradiction, that $n = x^2 + y^2$ is divisible by a prime $p \equiv 3 \bmod 4$ to an odd power k, and furthermore that this odd power is *minimal* (i.e. if $n' = x'^2 + y'^2$ is divisible by a prime $p' \equiv 3 \bmod 4$ to an odd power k', then $k \leq k'$). Such a minimal k exists since any nonempty set of positive integers has a minimal positive integer (i.e. the positive integers are well-ordered).

Now, $x^2 + y^2 \equiv 0 \mod p$. Notice that we cannot have $y \not\equiv 0 \mod p$, since in this case

$$x^2 \equiv -y^2 \mod p \Rightarrow \left(\frac{x}{y}\right)^2 \equiv -1 \mod p$$

which is a contradiction with Corollary 42.2. Thus $y \equiv 0 \bmod p$, which forces $x^2 \equiv 0 \bmod p$ and therefore $x \equiv 0 \bmod p$. Yet then $\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$ is the sum of two squares and is divisible by an prime $p \equiv 3 \bmod 4$ to an odd power strictly smaller than k (precisely, $k - 2$), which is a contradiction.

On the other hand, suppose that every prime divisor p of n with $p \equiv 3 \mod 4$ occurs to an even power in the prime factorization of n. Then the result follows from noticing that every prime of the form $p \not\equiv 3 \bmod 4$ is the sum of two squares, any square of a prime p^2 is the sum of two squares trivially $(0^2 + p^2)$, and the product of the sum of two squares is itself the sum of two squares via the following identity:

$$(x^2 + y^2)(x'^2 + y'^2) = (xx' + yy')^2 + (xy' - yx')^2.$$

□

Though we will not prove it here, Legendre and Gauss proved that a natural number is the sum of three squares if and only if it is not of the form $4^j(8k + 7)$ with j, k nonnegative integers. The necessity is trivial to prove since a square is congruent to $0, 1, 4 \bmod 8$, but we cannot prove the sufficiency without developing the theory of ternary quadratic forms (which we will not be doing).

In fact, any natural number n can be represented as the sum of four squares, though we will not prove it here. Key in the proof of this result is Euler's Identity for sums of four squares, which states that

$$\begin{aligned}(x^2 + y^2 + z^2 + w^2)(x'^2 + y'^2 + z'^2 + w'^2) = \\ (xx' + yy' + zz' + ww')^2 + (xy' - yx' + wz' - zw')^2 + \\ (xz' - zx' + yw' - wy')^2 + (xw' - wx' + zy' - yz')^2.\end{aligned}$$

Notice that this formula has the "same flavor" as the analogous identity on sums of two squares. Indeed, there is a deep algebraic reason for this. Both of these formulas can be thought as of as expressing the multiplicativity of a natural norm on some division algebra over the real numbers – for the sum of two squares, it is the complex numbers $\mathbb{C}$, and for the sum of four squares, it is the quaternions $\mathbb{H}$.

An interesting and related problem is Waring's problem. Formally, Waring's conjecture states that for any positive integer k, there exists a constant $s = s(k)$ so that any natural number n can be represented as the sum of s perfect kth powers of nonnegative integers. We define $g(k)$ to be the least such s that works – indeed $g(2) = 4, g(3) = 9, g(4) = 19$, etc. This was proven in 1909 by Hilbert and later in 1920 by Hardy and Littlewood via their now-famous "circle method" (which is of course discussed later in this paper).

7 Topics in Computational Number Theory

In this section, we'll speak about algorithms that are of interest both to computer scientists and number theorists. In particular, we'll offer ways to compute many of the objects we've spoken about earlier, and then apply our algorithms to the case of encryption schemes. For the sake of completeness, we also discuss quantum algorithms and post-quantum encryption, though these topics are decidely less number-theoretic.

7.1 The (Extended) Euclidean Algorithm

To explain the extended Euclidean algorithm, we will start with the ordinary Euclidean algorithm. In the ordinary Euclidean algorithm, we begin with two integers a and b (which for simplicity we will assume are non-negative), and attempt to find the greatest common divisor $\gcd(a, b)$.

Definition 52 (The Euclidean Algorithm)**.** Given two non-negative integers a and b, the *Euclidean algorithm* returns $\gcd(a, b)$. The computational complexity of this algorithm is $O(\log(a+b)^2)$, according to here.

Formally, we define two sequences: a "remainder sequence $\{r_i\}$" and a "quotient sequence $\{q_i\}$". We begin with initial conditions $r_0 = a$, $r_1 = b$, and define r_i, q_i inductively as the unique non-negative integers (given by the division algorithm) satisfying $r_{i-2} = r_{i-1}q_i + r_i$ and $r_i < r_{i-1}$. Since r_i is strictly decreasing, after a finite number of steps, there must exist some k such that $r_k = 0$. Then $\gcd(a, b)$ is r_{k-1}.

To see why $r_{k-1} = \gcd(a, b)$, notice that each new term of $\{r_i\}$ is a linear combination of the terms preceding them. Since we begin with initial terms a and b, this implies that each term of $\{r_i\}$ is a linear combination of a and b, and hence divides a and b. Furthermore, the final positive term of the sequence, r_{k-1}, is the smallest positive integer dividing a and b, hence the greatest common divisor of a and b.

Listing 1: A simple implementation of the Euclidean algorithm in Python

```
def euclidean_algorithm(a,b):
  r = [a,b]
  while True:
    q = r[0]//r[1]
    r = [r[1], r[0] - r[1]*q]
    if r[1] == 0:
      return r[0]
```

An important note is that the Euclidean algorithm is not actually the fastest known way to compute the greatest common divisor, because the operation of division is more complex than operations like addition, subtraction, or bitwise operations. Indeed, there exist other algorithms which are quicker, such as the *binary GCD algorithm*. This algorithm has the same computational complexity as the Euclidean algorithm but in practice uses less than half the bit operations (cite).

Definition 53 (Binary GCD)**.** Given two non-negative numbers a and b, apply the following rules:

1. $\gcd(0, a) = a$ and $\gcd(b, 0) = 0$.

2. If a and b are even, $\gcd(a,b) = 2\gcd(\frac{a}{2}, \frac{b}{2})$.
3. If a is even and b is odd, then $\gcd(a,b) = \gcd(\frac{a}{2}, b)$.
4. If a is odd and b is even, then $\gcd(a,b) = \gcd(a, \frac{b}{2})$.
5. If a and b are odd, then $\gcd(a,b) = \gcd(|a-b|, \min(a,b))$.

This algorithm recursively returns the greatest common divisor using just comparison, subtracting, and bitshifting (to multiply or divide by 2).

However, though the Euclidean algorithm is not the quickest practical algorithm, it's still worth discussing the Euclidean algorithm, because its "extension" helps us compute even more than the greatest common divisor, and will prove useful later.

Definition 54 (The Extended Euclidean Algorithm)**.** Given integers a and b, the *extended Euclidean algorithm* computes integers x and y such that

$$xa + yb = \gcd(a,b).$$

Notice that when a and b are coprime, then x is the inverse of $a \bmod b$, and y is the inverse of $b \bmod a$. Therefore, the extended Euclidean algorithm can be used to quickly (with the same computational complexity as the Euclidean algorithm) compute inverses mod n.

Now, recall that we define $r_0 = a$, $r_1 = b$, and r_i and q_i recursively as the unique non-negative integers such that $r_{i-2} = r_{i-1}q_i + r_i$ and $r_i < r_{i-1}$ (using the division algorithm). We also want to define sequences $\{x_i\}$ and $\{y_i\}$ such that $x_i a + y_i b = r_i$ for each i; then if $r_{k-1} = \gcd(a,b)$, $x = x_{k-1}$ and $y = y_{k-1}$.

To define $\{x_i\}$ and $\{y_i\}$, notice that $x_0 = 1$ and $y_0 = 0$ satisfy $x_0 a + y_0 b = r_0$. Similarly, $x_1 = 0$ and $y_1 = 1$ satisfy $x_1 a + y_1 b = r_1$. Therefore, these are the "initial conditions" for $\{x_i\}$ and $\{y_i\}$. Furthermore, if we assume $r_j = x_j a + y_j b$ holds for all $j < i$, then by applying $r_{i-2} = r_{i-1}q_i + r_i$, we find that

$$r_i = r_{i-2} - r_{i-1}q_i = (x_{i-2}a + y_{i-2}b) - (x_{i-1}a + y_{i-1}b)q_i = (x_{i-2} - x_{i-1}q_i)a + (y_{i-2} - y_{i-1}q_i)b$$

Hence, we define $x_i = (x_{i-2} - x_{i-1}q_i)$ and $y_i = (y_{i-2} - y_{i-1}q_i)$, and $r_i = x_i a + y_i b$ holds for all i.

Listing 2: A simple implementation of the extended Euclidean algorithm in Python

```
def extended_euclidean_algorithm(a,b):
  r = [a,b]
  x = [1,0]
  y = [0,1]
  while True:
    q = r[0]//r[1]
    r = [r[1], r[0] - r[1]*q]
    x = [x[1], x[0] - x[1]*q]
    y = [y[1], y[0] - y[1]*q]

    if r[1] == 0:
      return (r[0],x[0],y[0])
```

7.2 The Repeated Squaring Method

Besides computing inverses mod n, we will soon find that there are many practical reasons (for example, in cryptography) why one might want to compute a large power of an element mod n.

One might consider computing $a^k \bmod n$ by simple induction; take a^{k-1}, multiply by a, and reduce. However, this option is suboptimal: when k is large, this requires a large number of iterations (linear with k, and exponential with the number of digits of k). Therefore, there exists a smarter method:

Definition 55 (Repeated Squaring Method)**.** To compute $a^k \bmod n$, consider the binary representation of k: $\sum_{i=0}^{N} k_i 2^i$. Then, repeatedly square mod n to compute $a^{2^i} \bmod n$ for each $i \leq N$. Then $a^k \equiv a^{k_1 2^1} \cdots a^{k_N 2^N}$.

This algorithm is efficient because we only need to square a number $N-1$ times, and then only need to multiply $N+1$ numbers together. Indeed, everything we need to do has complexity at most $O(N^2)$, making the repeated squaring method polynomial in N, the number of bits of k.

As it turns out, not only will we encounter cases where this method is useful in our study of cryptography, but a very similar method will be defined in later dicussions on elliptic curves.

7.3 Primality Testing and Factorization

Definition 56 (Primality Test)**.** A *primality test* is a test for determining if a natural number n is prime. A *probabilistic* primality test does not prove that its input is prime, but rather demonstrates that it is likely to be prime by showing that it has many "prime-like" characteristics (which are usually computationally simple to check). On the other hand, a *deterministic* primality test does prove that its input is prime.

First, we will discuss a simple (but flawed) probabilistic primality test:

Definition 57 (Fermat Pseudoprime)**.** Suppose now that n is composite and odd, and choose an integer b which is coprime to n. Then, if $b^{n-1} \equiv 1 \bmod n$, we say that n is called a *Fermat pseudoprime at b*.

This name comes from the statement of Fermat's Little Theorem, which states that any prime p satisfies $b^{p-1} \equiv 1 \bmod p$ if $(b, p) = 1$. The probabilistic test that we do is finding a set of coprime bases b and testing $b^{n-1} \equiv 1 \bmod n$. If it ever fails, then we now that n is composite, whereas if it continues to succeed, we might suspect that n is prime. However, there is a major flaw with this reasoning:

Definition 58 (Carmichael Number)**.** A *Carmichael number* is a natural number n such that $b^{n-1} \equiv 1 \bmod n$ for all b coprime to n. The smallest example is of a Carmichael number is 651, but unfortunately for the Fermat primality test, there are infinitely many Carmichael numbers.

Proposition 56 (Characterizing Carmichael Numbers)**.** *n is a Carmichael number if and only if n is squarefree and for each prime $p \mid n$, $(p-1) \mid (n-1)$.*

Clearly, there are some flaws with this probabilistic test. Therefore, let's consider another such test:

Definition 59 (Jacobi Symbol)**.** Let n have prime factorization $p_1^{a_1} \cdots p_k^{a_k}$. Then the *Jacobi symbol of b mod n* is defined as so:

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right)^{a_1} \cdots \left(\frac{b}{p_k}\right)^{a_k}$$

where $\left(\frac{b}{p_i}\right)$ is the ordinary Legendre symbol for each i.

Definition 60 (Euler Pseudoprime)**.** Let n be composite and odd and let b be an integer such that $(b, n) = 1$. We call n an *Euler pseudoprime to the base b* if, with the Jacobi symbol, we have:

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \mod n \tag{3}$$

Just like Fermat pseudoprimes, this name comes from Euler's Criterion (Proposition 42), as if n is a prime then Euler's Criterion guarantees that this result holds. Therefore, if n ever fails this test, we know that it's composite. Like the Fermat primality test, there are composite Euler pseudoprimes; for example, 703 to the base 3. However, there is a major reason why the Euler primality test is superior:

Proposition 57. *There is no composite number n which is an Euler pseudoprime for every base b.*

Proof. Suppose n is square-free and has a prime divisor p. Then, let a be a quadratic nonresidue $\bmod p$, and b be a solution to the congruence $x \equiv a \bmod p$ and $x \equiv 1 \bmod \frac{n}{p}$, which exists by the Chinese Remainder Theorem. Then it is not difficult to check that n is not an Euler pseudoprime to the base b. On the other hand, if n is not square-free, then $p^2 \mid n$ for some prime p. Then one can easily check that n is not an Euler pseudoprime to the base $b = 1 + \frac{n}{p}$. □

Proposition 58. *The probability that a composite number n passes k trials with different random bases b is at most $\frac{1}{2^k}$. This does* not *mean that there is a probability of at most $\frac{1}{2^k}$ that it is composite. Instead, Bayesian probability using the approximate density of primes near n as a prior is the best way to approximate the chance that n is prime.*

Proof. If n is an Euler pseudoprime to bases b and b' then the multiplicative property of the Jacobi symbol guarantees it is not an Euler pseudoprime to the base bb'. Thus at most half of the b with $0 < b < n$ and (b, n) are bases which n is an Euler pseudoprime to, and the result follows. □

This concludes our discussion of primality testing. To learn more about primality testing (including deterministic tests), read this bachelor's project. In fact, there does exist a deterministic polynomial-time primality test, the AKS primality test. However, the AKS primality test is complex and beyond the scope of this discussion (though it is in the linked bachelor's project).

Next, we'll discuss two simple methods which are usually an improvement over the naive method of factoring. However, they are not a general efficient method, as their worst case scenarios can be quite inefficient.

Definition 61 (Fermat Factorization)**.** Suppose n is odd and $n = ab$ with $a \geq b > 0$. Then, $n = r^2 - s^2$ with $r = \frac{a+b}{2}$ and $s = \frac{a-b}{2}$. Conversely, if we can express n as $r^2 - s^2$, then $n = ab$ with $a = r + s$ and $b = r - s$. When a and b are close together, s is small, so r^2 will only be slightly bigger than n. Therefore, we let $r = \lfloor \sqrt{n} \rfloor, \lfloor \sqrt{n} \rfloor + 1, \lfloor \sqrt{n} \rfloor + 2, \ldots$ and check for each option if $r^2 - n$ is a perfect square s^2. If it is, we have a factorization of n as $(r + s)(r - s)$. Then, we might recursively factor $(r + s)$ and $(r - s)$.

However, Fermat factorization is not usually applied in such a direct manner. Instead, we try to find integers r, s such that $r^2 \equiv s^2 \bmod n$. Then $(r - s, n)$ and $(r + s, n)$ (if they are nonzero) are proper divisors of n. Notice that until $r \equiv s \equiv 0$, then at least one of these is guaranteed to be nonzero. Thus, to factor numbers, one may use this method instead of Fermat factorization. To implement this method efficiently and reliably, we define *Fermat bases*, covered in Section 9.4 of Baker's *A Comprehensive Course in Number Theory*.

Definition 62 (Pollard's $p - 1$ method)**.** Let n be a composite positive integer. If some prime factor p of n has the property that $p - 1$ has no large prime divisor, then there is a method that will almost always easily find p. Pollard's method is done as follows:

1. Choose an integer bound K.
2. Let k be divisible by all the integers not exceeding K (so $k = K!$ or $k = \text{lcm}(2, \ldots, K)$, for example).
3. For any integer a with $1 < a < n - 1$, we find $a^k \bmod n$ and compute $(a^k - 1, n)$.
4. If the result is nontrivial, we have found a factor of n. Otherwise, we will try again with different a, and if necessary change the integer bound K (usually increasing it) until we get the desired result.

To see why Pollar's $p - 1$ method works, consider the following. If k is divisible by all integers up to K, and $p - 1$ is divisible only by prime powers less than K, then $p - 1$ divides k. Hence, by Fermat's Theorem, we have $a^k \equiv 1 \bmod p$ for all integers a with $(a, p) = 1$. Hence $(a^k - 1, n)$ is divisible by p and is also a proper divisor of n unless $a^k \equiv 1 \bmod n$.

As an example, consider $n = 212899$. Let $K = 7$ and thus $k = 420$. Now we pick $a = 2$ and note $a^k = 2^{420} \equiv 54861 \mod n$ and $(54860, n) = 211$. Then division allows us to see that $n = 211 \times 1009$.

7.4 Encryption Using Modular Arithmetic

Two easy-to-understand encryptic methods are the Diffie-Hellman and RSA encryption processes. As you read, try to notice the places where the algorithms we discussed previously might be used.

Definition 63 (Diffie-Hellman Key Exchange)**.** Suppose Alice and Bob both publicly agree on a base c and a modulo p, usually such that c is a primitive root mod p. Alice chooses a secret number a and Bob chooses a secret number b. Then, they both compute $c^a \bmod p$ and $c^b \bmod p$ respectively, sharing the result with each other publicly. Finally, they compute $c^{ab} \bmod p$ privately, being the only ones who now know this number. This key can be used in any number of symmetric encryption schemes.

This process is secure because it is difficult for modern-day computers to find a given $c \bmod p$ and $c^a \bmod p$; this is called the *discrete logarithm problem*, and there is no known polynomial-time algorithm for solving it. Notice that the stipulation "mod p" is crucial; given c and c^a, it is quite easy for computers to calculate a to a very high accuracy with the ordinary logarithm. However, as the prime p has more and more digits (often upwards of 600), it is practically impossible to solve the *discrete* logarithm problem.

Definition 64 (RSA Encryption)**.** Suppose Alice chooses two large primes p and q and computes $pq = n$. It is not difficult for her to compute $\phi(n) = (p-1)(q-1)$, but an outsider would have difficulty doing this given only n (since they would have to factor n, which is very difficult if it has hundreds of digits).

Now, choose $m < \phi(n)$ with $(m, \phi(n)) = 1$. Let l be the smallest solution to $lm \equiv 1 \bmod \phi(n)$. The pair (n, m) form the *public key* and l forms the *private key*. Then, if someone wants to send you a message encoded as a number $0 < C \leq n$, they publicly send you $C^m \bmod n$. Then, you raise their message C^m to the lth power, netting $C^{ml} \equiv C^{1+k\phi(n)} \equiv C \bmod n$. Note that here we use Euler's Theorem, $C^{\phi(n)} \equiv 1 \bmod n$.

In any case, you have now recovered the decrypted text C while only receiving the cyphertext C^m. Furthermore, anybody seeking to find C from the cyphertext C^m would need to compute $\phi(n)$, which is quite difficult as no polynomial-time algorithm for factorization is known.

Interestingly, RSA is also symmetric in the sense that one can use the private key to send a message decryptable with the public key. This is an interesting method of identity verification, as the ability to encode a previously-agreed upon message is identical to the ability to decode a private message – since l and m are symmetrically inverses mod $\phi(n)$.

7.5 Defining Elliptic Curves

Let k be a field with characteristic not equal to 2 or 3. For the purposes of our discussion, we will define elliptic curves purely algebraically; a full definition would require a substantial amount of topology beyond the purposes of our discussion.

Definition 65 (Elliptic Curves over k)**.** An *elliptic curve* over a field k is the set of solutions $(x, y) \in k^2$ to an equation of the form $y^2 = x^3 + ax + b$, where $a, b \in k$ must satisfy the following requirement:

$$4a^3 + 27b^2 \neq 0.$$

This definition may initially seem contrived, but ultimately there are good reasons for each the choices we made in this definition. The fact that we restrict to equations of the form $y^2 = x^3 + ax + b$ is a product of the fact that any arbitrary cubic (degree 3) curve, that is, any equations of the form

$$Ay^3 + By^2x + Cyx^2 + Dx^3 + Ey^2 + Fxy + Gx^2 + Hx + Iy + J = 0$$

can be rearranged into an equation of the form $y^2 = x^3 + ax + b$ using changes in variables.

As for the choice to require $4a^3 + 27b^2 \neq 0$, this axiom is required to ensure the resulting curve is *non-singular*. A *singular point on an algebraic curve* $F(x, y)$ is a point where the partial (algebraic) derivatives $\frac{\partial F}{\partial x}$ and $\frac{\partial F}{\partial y}$ both vanish. It's significant because there is no unique tangent line to the curve at singular points; as we'll soon see, the existence of unique tangent lines is very important for the group law we will define on elliptic curves, so requiring the curve to be non-singular (i.e. to have to singular points) is not just natural, but necessary. Following are some images of non-singular (left) and singular (right) cubic curves:

Definition 66 (Point at Infinity)**.** For elliptic curve $y^2 = x^3 + ax + b$ over k, we append an ideal *point at infinity*, which we denote by 0. Geometrically, one can imagine the point at infinity as existing infinitely far above the origin, but formally speaking this is not part of the definition.

Definition 67 (Group Law)**.** We define the *group law on an elliptic curve* E by the following facts:

1. 0, the point at infinity, is the identity element, and we define $P+0 = P+0 = P$ for any point P on E.
2. The additive inverse of a point $P = (x, y)$ is the reflection of P across the x-axis: $-P = (x, -y)$.
3. Any three nonzero colinear points have zero sum; that is, if P, Q, and R are nonzero, then $P+Q+R = 0$.

Notice that (3) demonstrates how to add any two distinct nonzero points P and Q; find the third point R on E which lies on the line $\overline{PQ}$, and then $P + Q + R = 0$ implies $P + Q = -R$. Similarly, finding $P + P$ for any nonzero point P is also simple; take the tangent line to the curve at P, which intersects the curve at another point R, and then $P + P = -R$. This latter discussion makes it clear why we needed to define elliptic curves as nonsingular; otherwise, there would be a chance that $P + P$ would not be well-defined.

Proposition 59. *The group law on an elliptic curve E satisfies the axioms of a group.*

Proof. Trivial, left as an exercise to the reader. □

Theorem 60 (Adding Distinct Points)**.** *Given two distinct points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ on an elliptic curve E, either $x_P = x_Q$ and $y_P = -y_Q$ (so that $P + Q = 0$), or the slope of $\overline{PQ}$ is*

$$m = \frac{y_P - y_Q}{x_P - x_Q}$$

and the coordinates of the third point $R = (x_R, y_R)$ on E and $\overline{PQ}$ is

$$x_R = m^2 - x_P - x_Q \qquad y_R = y_P + m(x_R - x_P).$$

Then $P + Q = -R = (x_R, -y_R)$.

Proof. It suffices to check that R satisfies the cubic equation and P, Q, and R are distinct and aligned. □

Theorem 61 ($P + P$)**.** *Given a point $P = (x_P, y_P)$ on an elliptic curve E with equation $y^2 = x^3 + ax + b$, either $y_P = 0$ (in which case $P = -P$ so that $P + P = 0$), or the slope of the tangent line to E at P is*

$$m = \frac{3x_P^2 + a}{2y_P}$$

and then the other point $R = (x_R, y_R)$ on E and the tangent line to E at P is again

$$x_R = m^2 - x_P - x_Q \qquad y_R = y_P + m(x_R - x_P).$$

Then $P + P = -R = (x_R, -y_R)$.

Proof. It suffices to check that the point R satisfies the cubic equation, and that P and R are distinct and the only points on $\overline{PR}$ also on E. □

Definition 68 (Double and Sum Algorithm)**.** Suppose that we are given a point P on an elliptic curve E, and a large positive integer c. Then, computing cP naively (by adding P a total of c times) is inefficient; instead, we use an algorithm analogous to the Repeated Squaring Method (Definition 55) to compute cP.

Namely, suppose that c has binary expansion $\sum_{i=0}^{n} c_i 2^i$. Then, we compute $2P = P + P$, $4P = 2P + 2P$, $8P = 4P + 4P$, and so on until we get to $2^i P$. Then it simply suffices to compute

$$cP = c_0(P) + c_1(2P) + c_2(4P) + \cdots + c_i(2^i P).$$

Definition 69 (The Discrete "Logarithm" Problem on Elliptic Curves)**.** The normal discrete logarithm problem is the task of finding b given $a \bmod p$ and $a^b \bmod p$. The *discrete logarithm problem on elliptic curves* is the task of finding the constant c given a point P and cP on an elliptic curve over a finite field (usually $\mathbb{F}_p$, the field of integers modulo a prime p, for $p > 3$).

Just like the ordinary discrete logarithm problem, the discrete logarithm problem on elliptic curves is thought to be computationally "hard", and no algorithm that can solve it quickly is known. The further benefit of using elliptic curves is that the discrete logarithm problem for elliptic curves is thought to be even more difficult, and therefore we can use smaller keys to get the same amount of security. Consider, for example, the National Institute of Standards and Technology's table of comparative security, which finds that

Bits of Security	Bits in Public Key of DSA	Bits in the Key of ECDSA
80	1024	160-223
112	2048	224-255
128	3072	256-383
192	7680	384-511
256	15360	512+

Table 1: Encryption Schemes with Comparable Strength

ECDSA is a type of elliptic-curve cryptography which we will discuss in the next section.

7.6 Elliptic Curve Cryptography

1. Finding order of elliptic curve 2. Finding period of elements 3. Finding element with a large period 4. Verifiably random 5. Public and private keys 6. ECDH 7. ECDSA

8 Miscellaneous

Following are a few various number-theory related digressions:

8.1 Perfect Numbers and Mersenne Primes

Definition 70 (Perfect Numbers)**.** A natural number n is *perfect* if the sum of the divisors of n is $2n$; that is, if $\sigma(n) = 2n$.

The two smallest perfect numbers are 6 and 28. It is an open question whether or not there are any odd perfect numbers (as all the ones we've found are even, and papers have checked up to 10^{1500}), as well as whether or not there are infinitely many perfect numbers.

Definition 71 (Mersenne Primes)**.** A prime number $p \in \mathbb{Z}^+$ is called a *Mersenne prime* if $p = 2^q - 1$ for some prime number q. It is an open question if there are infinitely many Mersenne primes.

It turns out there is an interesting correspondence between Mersenne primes and even perfect numbers. To prove this correspondence, we will need the following lemma on divisibility:

Lemma 62 (Power Divisibility)**.** *Suppose x is an integer, and m and n are integers such that $m \mid n$. Then,*

$$x^m - 1 \mid x^n - 1.$$

Proof. Notice that the following polynomial identity holds under the assumption that m divides n.

$$X^n - 1 = (1 + X^m + X^{2m} + \cdots + X^n)(X^m - 1).$$

By substituting an integer x for the indeterminate X, we notice that $x^n - 1$ is an integer multiple of $x^m - 1$. □

Proposition 63 (Perfect Numbers and Mersenne Primes)**.** *An even number is perfect if and only if it has the form $2^{p-1}(2^p - 1)$, where both p and $2^p - 1$ are primes. In other words, any even perfect number gives arise to a Mersenne prime (the unique odd prime factor of the even perfect number is a Mersenne prime), and any Mersenne prime $2^p - 1$ gives rise to an even perfect number, namely $2^{p-1}(2^p - 1)$.*

Proof. To prove "if", suppose that $n = 2^{p-1}(2^p - 1)$, where p and $2^p - 1$ are prime. Then by Proposition 17, the σ function is multiplicative, so

$$\sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\sigma(2^p - 1) = (1 + 2 + \cdots + 2^{p-1}) \cdot (2^p) = (2^p - 1)(2^p) = 2n.$$

To prove "only if", suppose that n is even and $\sigma(n) = 2n$. Then, we can express $n = 2^k m$, where k and m are positive integers and m odd. Then,

$$2^{k+1}m = 2n = \sigma(n) = \sigma(2^k m) = (2^{k+1} - 1)\sigma(m)$$

In summary, $2^{k+1}m = (2^{k+1} - 1)\sigma(m)$. Since 2^{k+1} and $2^{k+1} - 1$ are coprime, we may conclude that $\sigma(m) = 2^{k+1}l$ and $m = (2^{k+1} - 1)l$ for some positive integer l. Notice that l also satisfies $\sigma(m) = m + l$. Yet if $l > 1$, then since l divides m, $\sigma(m) \geq m + l + 1$, which contradicts $\sigma = m + 1$. Hence $l = 1$, so $\sigma(m) = m + 1$, implying that m is prime and equal to $2^{k+1} - 1$. Then, by Lemma 62, we must have that $k + 1 = p$ is prime. Yet then $n = 2^{p-1}(2^p - 1)$ is such that p and $2^p - 1$ is also prime, as desired. □

8.2 Diophantine Approximations

One topic of interest is the approximation of arbitrary real numbers by rational numbers with sufficiently small denominators. A basic result on the matter follows from the Pigeonhole Principle.

Theorem 64. *Let r be a real number, and take an integer $N > 1$. Then there exist integers p and q with $0 < q < N$ such that $|qr - p| \leq \frac{1}{N}$.*

Proof. Let $\{x\} = x - \lfloor x \rfloor$ for each real number x. Then, consider the $N+1$ numbers $0, 1, \{r\}, \{2r\}, \ldots, \{(N-1)r\}$. These numbers all lie in the set $[0, 1]$, so by the Pigeonhole Principle at least two of them must lie in one of the N intervals $[0, \frac{1}{N}], [\frac{1}{N}, \frac{2}{N}], \ldots, [\frac{N-1}{N}, 1]$. Then, the difference of these numbers has the form qr (for some $0 < q < N$) and has fractional part within $\frac{1}{N}$ of 0. Hence there exists an integer p such that $|qr - p| \leq \frac{1}{N}$, as desired. □

Corollary 64.1 (Dirichlet's Theorem)**.** *Take a real number r, and another real number $N \geq 1$. Then there exist integers p and q such that $0 < q \leq N$ and*

$$|qr - p| < \frac{1}{N}.$$

Proof. Follows trivially by using Theorem 64 on $\lfloor N \rfloor + 1$, as it will find integers p and q such that $0 < q < \lfloor N \rfloor + 1$ (whence $0 < q \leq N$) such that $|qr - p| \leq \frac{1}{\lfloor N \rfloor + 1} < \frac{1}{N}$. □

Corollary 64.2. *Notice that p and q can be chosen to be relatively prime (since if they have a common factor, dividing it out gets a strictly better result). Therefore, when r is irrational, there are infinitely many distinct rational numbers $\frac{p}{q}$ such that*

$$\left| r - \frac{p}{q} \right| < \frac{1}{q^2}$$

Proof. For any integer $N > 1$, there are coprime integers p, q with $\left| r - \frac{p}{q} \right| \leq \frac{1}{Nq} < \frac{1}{q^2}$. Furthermore, if r is irrational, then the rational generated by considering $N' > \frac{1}{|qr-p|}$ will be new $\frac{p'}{q'}$. Therefore, we can inductively generate an infinite list of rational numbers that closely approximate r. □

Note this is not generally true when r is rational.