Number Theory *

Zhiyuan Bai

Compiled on September 18, 2022

This document serves as a set of revision materials for the Cambridge Mathematical Tripos Part II course *Number Theory* in Michaelmas 2020. However, despite its primary focus, readers should note that it is NOT a verbatim recall of the lectures, since the author might have made further amendments in the content. Therefore, there should always be provisions for errors and typos while this material is being used.

Contents

*Based on the lectures under the same name taught by Dr. J. Wolf in Michaelmas 2020.

0 Introduction

Number theory studies the properties of integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ and rational numbers $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z}, q \neq 0\}$. Mathematicians have been thinking about these numbers since very early stages of humanity. Many problems were asked and answered. It would be pretty much impossible to ask for a full introduction to every possible area of number theory, but we shall present a few standing conjectures that will motivate us throughout the course (and indeed in further pursuit of number theory).

Conjecture 0.1 (Twin Prime Conjecture)**.** There exists infinitely many primes p such that $p+2$ is also prime.

The most recent result on this problem was obtained in 2013 and says there are infinitely many primes p such that $\{p+2, p+4, \ldots, p+246\}$ contains a prime.

Conjecture 0.2 (Riemann Hypothesis)**.** Let $\pi(x)$ be the number of primes that's at least x and

$$\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\log t}$$

Then

$$|\pi(x) - \mathrm{Li}(x)| \leq \sqrt{x} \log x$$

for all $x \in \mathbb{Z}_{\geq 3}$.

In 2016, it was proved that there are constants c, C such that

$$|\pi(x) - \mathrm{Li}(x)| \leq \frac{Cx}{(\log x)^{3/4}} e^{-c\sqrt{\log x}}$$

for all $x \geq 229$.

Conjecture 0.3. There is a polynomial-time algorithm that factorises $N = pq$ where p, q are primes.

The encryption method RSA depends on this conjecture being false.
In 2002, it was proved that testing whether or not a given integer is prime can be done in polynomial time.
Works towards these conjectures often involves sophisticated mathematical theories, but in this course we shall only cover elementary methods, but these will get us quite a long way.

1 Euclid's Algorithm

Proposition 1.1. *Given $a, b \in \mathbb{Z}$ with $b > 0$, there exists $q, r \in \mathbb{Z}$ with $a = bq + r$ and $0 \leq r < b$.*

Proof. Let $S = \{a - nb : n\mathbb{Z}\}$, then S contains some nonnegative integer. Let $r \geq 0$ be the least nonnegative integer that is contained in S, then $r < b$, because otherwise $r - b \in S$ would be nonnegative and smaller than r. So $a - qb = r$ for some $q \in \mathbb{Z}$, or $a = qb + r$. □

Definition 1.1. If $r = 0$, we write $b \mid a$ ("b divides a"), otherwie we write $b \nmid a$.

Given $a_1, \ldots, a_n \in \mathbb{Z}$ not all zero, let $I = \{\lambda_1 a_1 + \cdots + \lambda_n a_n : \lambda_i \in \mathbb{Z}\}$. Then for any $a, b \in I, l, m \in \mathbb{Z}$, then $la + mb \in I$.

Lemma 1.2. *$I = d\mathbb{Z} = \{md : m \in \mathbb{Z}\}$ for some $d > 0$.*

Proof. Let d be the least positive element in I, then $d\mathbb{Z} \subset I$. Conversely, if $a \in I$, write $a = qd + r$ for some $0 \leq r < a$. If $r = 0$, then $a \in d\mathbb{Z}$. Otherwise, $r = a - qd \in I$ is positive and smaller than d, contradiction. □

In particular, $d \mid a_i$ for all i; Conversely, if $c \mid a_i$ for all i, then $d\mathbb{Z} = I \subset c\mathbb{Z}$, hence $c \mid d$.

Definition 1.2. We write $d = \gcd(a_1, \ldots, a_n) = (a_1, \ldots, a_n)$ and say d is the greatest common divisor of $a_1, \ldots, a_n$.

Corollary 1.3. *Suppose $a, b, c \in \mathbb{Z}$ and a, b not both 0. There exists $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if $(a, b) \mid c$.*

Proposition 1.4 (Euclid's Algorithm)**.** *Suppose $a > b = r_0 > 0$. We can apply the division algorithm repeatedly to get*

$$\begin{aligned} a &= q_1 r_0 + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k + 0 \end{aligned}$$

where $0 < r_i < r_{i-1}$ for $i \leq k$. Then $r_k = (a, b)$.

Proof. Note that $r_k \mid r_0$ and $r_k \mid a$, so $r_k \leq (a, b)$. Note also that any m with $m \mid a$ and $m \mid b$ also divides r_k, hence $(a, b) \leq r_k$, so $(a, b) = r_k$. □

This also allows us determine $x, y \in \mathbb{Z}$ such that $d = (a, b) = ax + by$ ("Bezout's identity") by repeated substitution.

Example 1.1. Let $a = 34, b = 25$, then Euclid's algorithm becomes

$$\begin{aligned} 34 &= 1 \times 25 + 9 \\ 25 &= 2 \times 9 + 7 \\ 901 &\times 7 + 2 \\ 7 &= 3 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

So $1 = \gcd(34, 25)$. Working backwards gives $-11 \times 34 + 15 \times 25 = 1$.

Definition 1.3. An integer $n > 1$ is prime if its only positive divisors are 1 and n. Otherwise, it is composite.

Lemma 1.5. *Let p be a prime, let $a, b\mathbb{Z}$, then $p \mid ab$ iff $p \mid a$ or $p \mid b$.*

This is so not true for composite numbers.

Proof. The "if" direction is clear. Conversely, suppose $p \mid ab$ yet $p \nmid a$, then $(a, p) \neq p$ but $(a, p) \mid p$ and p is prime, so $(a, p) = 1$, therefore there are some integers n, y such that $ax + py = 1$. Now $b = b(ax + py) = x(ab) + (by)p \implies p \mid b$. □

Theorem 1.6 (Fundamental Theorem of Arithmetic)**.** *Every $n > 1$ can be written a a product of primes. Furthermore, this is unique up to reordering.*

Proof. Existence follows easily by strong induction. For uniqueness (which, hey, also follows from strong induction) suppose there is an integer with two distinct factorisations even with reordering. Let n be the least such integer. Say $n = p_1 \cdots p_s = q_1 \cdots q_r$ with all p_i, q_j prime. Then $p_1 \mid q_1 \cdots q_r$, so there is some j such that $p_1 \mid q_j$, which means $p_1 = q_j$ since q_j is prime. WLOG $j = 1$, then $n/p_1 = p_2 \cdots p_s = q_2 \cdots q_r$, contradicting minimality of n. □

Remark. By collecting multiplicity we can write any integer in the form $\prod_i p_i^{e_i}$ for some distinct primes p_i and $e_i \in \mathbb{Z}_{\geq 0}$. If we write $m = \prod_i p_i^{\alpha_i}, n = \prod_i p_i^{\beta_i}$ with p_i distinct primes, then $(m, n) = \prod_i p_i^{\min\{\alpha_i, \beta_i\}}$. This being said, it's much more efficient to compute gcd's with Euclid's algorithm than with factorisation.

Definition 1.4. An algorithm with input integer $N > 0$ is said to run in polynomial time if it completes after at most $C(\log N)^k$ many "elementary" operations for some constants $c, k > 0$. If the algorithm takes input $N_1, \ldots, N_s$, then the algorithm is said to run in polynomial time if it completes in at most $c(\max_i \log(N_i))^k$ operations for some constants c, k.

Example 1.2. Addition and multiplication run in polynomial time.
Euclid's algorithm also runs in polynomial time.

How about factorisation? Conjecture 0.3 hasn't been solved, so we don't know if there exists a polynomial-time algorithm for that. But it shouldn't be surprising that the obvious algorithm (trial division by integers at most $\sqrt{N}$) cannot be done in polynomial time. Indeed, if $N = pq$ with p, q prime, each with 50 digits, then trial division for N would take about 6×10^{39} years assuming we can do 2^9 divisions per second.
We will see more efficient division algorithms later, but none of them can be done in polynomial time. There's even a world record of factorising a 232 digit number that uses hundreds of computers and almost two years of computing time.
We also stated Conjecture 0.1, which would be silly if there weren't infinitely many primes, so let's review this theorem of Euclid.

Theorem 1.7. *There are infinitely many primes.*

Proof. For any $N > 1$, let p be the largest prime that's at most N, then any prime factor of $M = 2 \times 2 \times 5 \times \cdots \times p + 1$, then $q > N$. This means that primes can get arbitrarily large, i.e. there are infinitely many of them. □

2 Congruences

2.1 Modular Inverses

Definition 2.1. Let $n \geq 1$ be an integer, we write $a \equiv b \pmod{n}$ ("a is congruent to b modulo n") if $n \mid a - b$.

This defines an equivalence relation on $\mathbb{Z}$. We write $\mathbb{Z}/n\mathbb{Z}$ for the set of equivalence class $a + n\mathbb{Z}$. It is easu to check that the opersations $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}, (a + n\mathbb{Z}) \times (b + n\mathbb{Z}) = ab + n\mathbb{Z}$ are well-defined.

Lemma 2.1. *Let $a \in \mathbb{Z}$, then the followings are equivalent:*
(i) $(a, n) = 1$.
(ii) $\exists b\mathbb{Z}, ab \equiv 1 \pmod{n}$.
(iii) $a + n\mathbb{Z}$ *is a generator of* $(\mathbb{Z}/n\mathbb{Z}, +)$.

If these conditions hold, we say b is a multiplicative inverse to a.

Proof. (i) $\implies$ (ii): As $(a, n) = 1$, there exists $b, c \in \mathbb{Z}$ such that $ab + cn = 1$, i.e. $ab \equiv 1 \pmod{n}$.
(ii) $\implies$ (i): The condition means that there is an integer k with $ab - 1 = kn$, i.e. $ab - kn = 1 \implies (a, n) = 1$. (ii) $\implies$ (iii): For any k, the sum of bk copies of a is $a + \cdots + a = bka = abk \equiv k \pmod{n}$. □

Definition 2.2. We write $(\mathbb{Z}/n\mathbb{Z})^\times$ for the set of units (i.e. elements that satisfies the conditions in the preceding lemma) in $\mathbb{Z}/n\mathbb{Z}$.

Definition 2.3. $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ is called Euler's totient function (with $\varphi(1) = 1$ by convention).

Remark. (i) φ is multiplicative, i.e. if $(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.
(ii) if $n > 1$, $\mathbb{Z}/n\mathbb{Z}$ is a field iff $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z}) - \{0\}$, which happens precisely when n is prime. In this case, $\varphi(n) = n - 1$.

Corollary 2.2. *Let G be a cyclic group of order $n \geq 1$, then* $\varphi(n) = |\{g \in G : \mathrm{ord}(g) = n\}|$.

Proof. $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$. □

Theorem 2.3 (Euler-Fermat)**.** *If $a, n \in \mathbb{Z}$ have $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Proof. By Lagrange's theorem (on groups), the order of a in the multiplicative group $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ divides $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$. □

And when $n = p$ is a prime,

Theorem 2.4 (Fermat's little Theorem)**.** *If $a, p \in \mathbb{Z}$ with p prime, then $a^p \equiv a \pmod{p}$.*

Proof. The case $p \mid a$ is trivially true; The other case follows from the Euler-Fermat and the fact that $\varphi(p) = p - 1$. □

2.2 System of Linear Congruences

Example 2.1. We want to find $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv 4 \pmod 7 \\ x \equiv 5 \pmod{12} \end{cases}$$

Observe first that if we have a solution to the first congruence, then we can add to it anything that is congruent to 0 modulo 7 while still keeping it a solution to the congruence. Moreover, if we have a solution to $u \equiv 1 \pmod 7$, then $4u$ will be a solution to the first congruence.
Consequently, if we can find $u, v \in \mathbb{Z}$ such that

$$\begin{cases} u \equiv 1 \pmod 7 \\ u \equiv 0 \pmod{12} \end{cases}, \begin{cases} v \equiv 0 \pmod 7 \\ v \equiv 1 \pmod{12} \end{cases}$$

Then $4u + 5v$ is a solution to the original system.
How would we find u, v? Note that $(7, 12) = 1$, so there are integers m, n such that $7m + 12n = 1$, then $u = 12n, v = 7n$ straight up works. Indeed, we can take $n = 3, m = -5$ which gives $u = 36, v = -35$, so one solution to the system is given by $4u + 5v = -31$. In fact, the complete set of solutions is $\{x \equiv -31 \pmod{84}\}$.

Generalising this method gives

Theorem 2.5 (Chinese Remainder Theorem)**.** *Suppose $m_1, \ldots, m_k$ are pairwise coprime positive integers. Then for any $a_1, \ldots, a_k \in \mathbb{Z}$, there is a solution $x \in \mathbb{Z}$ to the system*

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ & \vdots \\ x & \equiv a_k \pmod{m_k} \end{cases}$$

Moreover, x is unique modulo $M = \prod_i m_i$.

Remark. Indeed, whenever x is a solution to the system, $x + tM$ would also be a solution for any $t \in \mathbb{Z}$, so the full set of solution is just $x + M\mathbb{Z}$.

Proof. Uniqueness is straightforward: If x, y satisfies the system, then $m_i \mid x - y$ for all i, therefore $M \mid x - y$ since there is no prime that divides two distinct m_i's.
As for uniqueness, write $M_i = M/m_i$, then $(m_i, M_i) = 1$ for all i. Therefore for each i there is some b_i such that $M_i b_i \equiv 1 \pmod{m_i}$. We also have $M_i b_i \equiv 0 \pmod{m_j}$ for all $j \neq i$. Take $x = \sum_i a_i b_i M_i$. □

We can take a more algebraic point of view: If $m_1, \ldots, m_k$ are pairwise coprime and $M = \prod_i m_i$, then what the theorem is saying is that the map $\theta : \mathbb{Z}/M\mathbb{Z} \mapsto (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_k\mathbb{Z})$ via product of reduction is an isomorphism of rings. In particular, if $n = \prod_i p_i^{\alpha_i}$ where $p_1, \ldots, p_k$ are distinct primes, then $\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$. A warning to be put here is that we cannot in general split up the prime powers since e.g. $\mathbb{Z}/4\mathbb{Z}$ is not isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.
Sometimes we need instead a refinement of Chinese Remainder Theorem.

Lemma 2.6. *If in addition that $(a_i, m_i) = 1$ for all i, then any solution to the system must be coprime to M.*

Proof. Suppose the solution x has $(x, M) > 1$, then there is a prime p that divides both x and M. But M is the product of all m_i's, so there exists an i such that $p \mid m_i$, but this would mean that $p \mid a_i$, hence $(a_i, m_i) \neq 1$. □

Algebraically, this means that $(\mathbb{Z}/M\mathbb{Z})^\times \cong (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times \mathbb{Z}/(m_k\mathbb{Z})^\times$ as groups. In particular, they have the same order.

Corollary 2.7. *If $m_1, \ldots, m_k$ are pairwise coprime and $M = \prod_i m_i$, then $\varphi(M) = \prod_i \varphi(m_i)$.*

Definition 2.4. A function $f : \mathbb{Z}_{>0} \to \mathbb{C}$ is called multiplicative if for any coprime m, n we have $f(mn) = f(m)f(n)$.
It is totally multiplicative if $f(mn) = f(m)f(n)$ for any pair of positive integers m, n.

Example 2.2. $\varphi(n), \tau(n) = |\{d : d \mid n\}|, \sigma(n) = \sum_{d|n} d, \sigma_k(n) = \sum_{d|n} d^k$ are multiplicative, but none of them is totally multiplicative.

Note that $\sigma_1 = \sigma, \sigma_0 = \tau$, but it is not quite obvious that σ_k is multiplicative. How do we show this? Expansion is easy, but we might want to go a step further.

Lemma 2.8. *If f is a multiplicative, so is $g : n \mapsto \sum_{d|n} f(d)$*

Proof. If $(m, n) = 1$, then the divisors of the product mn are precisely the integers of the form $d_1 d_2$ where $d_1 \mid m, d_2 \mid n$ and $(d_1, d_2) = 1$. So

$$g(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) = \sum_{d_1|m} \sum_{d_2|n} f(d_1)f(d_2) = g(m)g(n)$$

as desired. □

Example 2.3. Let f be the multiplicative function $n \mapsto n^k$, then $g(n) = \sigma_k(n) = \sum_{d|n} d^k$ must also be multiplicative.

We will see later that this operation can actually be reversed.

Theorem 2.9. *(i) If p is prime and $m \in \mathbb{N}$, then $\varphi(p^m) = p^m(1 - p^{-1})$.*
(ii) $\varphi(n) = n \prod_{p|n}(1 - p^{-1})$ for any n.
(iii) $\sum_{d|n} \varphi(n) = n$.

Proof. (i) can be calculated from definition and (ii) follows from the multiplicity of n.
As for (iii), note that $g(n) = \sum_{d|n} \varphi(d)$ coincides with the identity at any prime power and is multiplicative by the preceding lemma, hence $g(n) = n$ for all n. □

2.3 Polynomial Congruences

Example 2.4. 1. $x^2 + 2 \equiv 0 \pmod 5$ has no solutions.
2. $x^3 + 1 \equiv 0 \pmod 7$ has thee solutions $3, 5, 6$.
3. $x^2 - 1 \equiv 0 \pmod 8$ has four solutions $1, 3, 5, 7$.

You should indeed be startled by the last example: The polynomial $x^2 - 1$ has degree 2, yet has four roots in $\mathbb{Z}/8\mathbb{Z}$.

Definition 2.5. Let R be a commutative ring, we define $R[X]$ be the set of finite formal sums $a_0 + \cdots + a_n X^n$ for $a_n \in R$. This is known as the polynomial ring of one variable over R.

Remark. Two polynomizals are equal if and only if their coefficients are equal. However, the functions represented by distinct polynomials can be the same. Take $R = \mathbb{Z}/p\mathbb{Z}$, then $X^p - X$ and 0 are distinct elements of $R[X]$ but they evaluated to the same function $R \to R$.

Proposition 2.10 (Division Algorithm)**.** *Let $f, g \in R[X]$ and suppose $m = \deg g > 0$ and that the leading coefficient of g has an inverse in R, then there are some $q, r \in R[X]$ such that $f = qg + r$ with $\deg r < m$.*

Proof. We proceed by induction on $n = \deg f$. The case where $\deg f < \deg g$ is obvious ($q = 0, r = f$). Suppose $\deg f \geq \deg g$, we write $f = aX^n + \cdots, g = bX^m + \cdots$, then $f' = f - ab^{-1}X^{n-m}g$ has degree strictly less than n, so there is some q', r such that $f' = q'g + r$ and $\deg r < \deg g$ by the induction hypothsis. Then $f = (ab^{-1}X^{n-m} + q')g + r$ which is what we wanted. □

Theorem 2.11 (Remainder Theorem)**.** *Suppose $f \in R[X], \alpha \in R$, then $f(X) = (X - \alpha)q(X) + f(\alpha)$ for some $q \in R[X]$.*

Proof. $f(X) = (X-\alpha)q(X)+r(X)$ for some r such that $\deg r < \deg(X-\alpha) = 1$. This means that r is constant. Putting in $X = \alpha$ gives $r = f(\alpha)$. □

Definition 2.6. A commutative ring R is an integral domain if for any $a, b \in R$ with $ab = 0$, either $a = 0$ or $b = 0$.

Example 2.5. $\mathbb{Z}$ and $\mathbb{Q}$ are integral domains. $\mathbb{Z}/N\mathbb{Z}$ is an integral domain if and only if N is prime.

Theorem 2.12. *Let R be an integral domain, and let $f \in R[X]$ be a nonzerpo polynomial of degree $n \geq 0$, then f has at most n distinct roots in R.*

Proof. We shall prove this by induction on n. The case $n = 0$ is trivial. For $n > 0$, if f has no roots when we are automatically done. Otherwise, f has some root $\alpha \in R$, then $f(X) = (X-\alpha)q(X)$ by remainder theorem. Then any root of f must either be α or a root of q since R is an integral domain. The induction hypothesis then implies that f has at most $1 + \deg q = 1 + \deg f - 1 = \deg f$ distinct roots. □

Theorem 2.13 (Lagrange)**.** *Let p be a prime and let $f(X) = a_0 + \cdots a_n X^n$. Suppose $p \nmid a_n$, then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n solutions modulo p.*

Example 2.6. Let p be a prime and let $f(X) = X^{p-1} - 1 - \prod_{a=1}^{p-1}(X - a)$, then f has $p - 1$ roots $1, \ldots, p - 1$ but its degree is at most $p - 2$, hence $f = 0$. In particular, $0 \equiv f(0) \equiv -1 - (p-1)! \pmod{p}$ which is Wilson's theorem.

2.4 Primitive Roots

Example 2.7. 3 generates $(\mathbb{Z}/7\mathbb{Z})^\times$, so $(\mathbb{Z}/7\mathbb{Z})^\times$ is a cyclic group of order 6.

Theorem 2.14. *If p is a prime, then $G = (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.*

Proof. Let N_d be the number of elements of G of order d, then we have

$$\sum_{d|p-1} N_d = |G| = \varphi(p) = p - 1 = \sum_{d|p-1} \varphi(d)$$

If G is not cyclic, then $N_{p-1} = 0 < \varphi(p-1)$, so there is some $d < p-1$ such that $N_d > \varphi(d) \geq 0$. Fix this d and let α be an element of order d (which exists since $N_d > 0$), then $\langle\alpha\rangle = \{1, \alpha, \cdots, \alpha^{d-1}\} \leq G$ is cyclic of order d, therefore has exactly $\varphi(d)$ elements of order d. But $N_d > \varphi(d)$, so there must be an element of order d in G which is not contained in $\langle\alpha\rangle$, therefore $X^d - 1$ has at least $d+1$ roots in $\mathbb{Z}/p\mathbb{Z}$, contradiction. □

Definition 2.7. A positive integer g is called a primitive root modulo n if it generates $(\mathbb{Z}/n\mathbb{Z})^\times$.

Example 2.8. Take $p = 19$. letb d be the order of 2 in $(\mathbb{Z}/19\mathbb{Z})^\times$. Note that $d \mid \varphi(19) = 18$, so either $d = 18$ or s divides one of 6 and 9. But neither $2^6 - 1$ nor $2^9 - 1$ is divisible by 19, hence necessarily $d = 18$, i.e. 2 is a primitive root modulo 19.

There are immense applications of primitive roots in cryptography, but we don't have time to talk about those here.
Naturally, there are some unsolved problems about primitive roots.

Conjecture 2.1 (Artin)**.** Given any $g \geq 1$, there exists infinitely many primes p for which g is a primitive root.

It is unsolved, but it has been proved that there exists infinitely many primes for which one of $2, 3, 5$ is a primitive root.
Another interesting problem is how large would the smallest primitive root modulo p be. We can prove that there is a constant c such that it is bounded by $cp^{1/4+\epsilon}$ for all $\epsilon > 0$. If the generalised Riemann hypothesis is assumed, then we can get a bound of $c \log^6 p$ for some constant c.
How about $(\mathbb{Z}/N\mathbb{Z})^\times$ when N is not prime? Let's not wander too far from our original result – let's start with prime powers first. Powers of 2 are kinda bad for this purpose.

Example 2.9. Every element in $(\mathbb{Z}/8\mathbb{Z})^\times = \{\pm 1, \pm 3\}$ has order 1 or 2, hence it cannot be cyclic. Also, we have the surjective homomorphism $\theta : (\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times$ via reduction, which means that none of $(\mathbb{Z}/2^k\mathbb{Z})^\times$ can be cyclic.

However, if one takes an odd prime, then

Theorem 2.15. *If $p > 2$ is prime, $k \geq 1$ and $y \in \mathbb{Z}$, then:*
(i) If $x \equiv 1 + p^k y \pmod{p^{k+1}}$, then $x^p \equiv 1 + p^{k+1} y \pmod{p^{k+2}}$.
(ii) $(1 + py)^{p^k} \equiv 1 + p^{k+1} y \pmod{p^{k+2}}$

Proof. It is clear that (i) implies (ii). To prove (i), we expand

$$\begin{aligned}(1+p^k y)^p &= \sum_{j=0}^{p}\binom{p}{j}(p^k y)^j = 1 + p^{k+1}y + \sum_{j=2}^{p-1}\binom{p}{j}(p^k y)^j + p^{kp}y^p \\ &\equiv 1 + p^{k+1}y \pmod{p^{k+2}}\end{aligned}$$

which implies the result. □

Lemma 2.16. *Let $p > 2$ be an odd prime and $k \geq 1$. If g is a primitive root modulo p and $g^{p-1} \not\equiv 1 \pmod{p^2}$, then g is a generator of $(\mathbb{Z}/p^k\mathbb{Z})^\times$.*

Proof. The case $k = 1$ has already been proved. Assume henceforth that $k \geq 2$. Let d be the order of g in $(\mathbb{Z}/p^k\mathbb{Z})^\times$, then $d \mid \varphi(p^k) = p^{k-1}(p-1)$, so if g is not a generator of $(\mathbb{Z}/p^k\mathbb{Z})^\times$, then either $d \mid p^{k-2}(p-1)$ or $d = p^{k-1}e$ for some $e \mid p-1$ and $e < p-1$.
If it were the former, then $g^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$. The condition means that there is some y not divisible by p such that $g^{p-1} = 1 + py$. By part (ii) of the preceding theorem, we have $g^{p^{k-2}(p-1)} \equiv (1+py)^{p^{k-2}(p-1)} \equiv (1+p^{k-1}y)^{p-1} \equiv 1 + (p-1)p^{k-1}y \not\equiv 1 \pmod{p^k}$, a contradiction.
If we were in the latter case, then $g^{p^{k-1}e} \equiv 1 \pmod{p^k}$. But $g^{p^{k-1}} \equiv g \pmod{p}$ by Fermat's little theorem, so $g^{p^{k-1}e} \equiv g^e \not\equiv 1 \pmod{p}$, consequently $g^{p^{k-1}e} \not\equiv 1 \pmod{p^k}$, contradiction. □

Example 2.10. We have seen that 3 is a primitive root modulo 7. Also, $3^6 - 1 = 7 \times 104$ is not divisible by 7^2, so the lemma implies that 3 is a primitive root modulo 7^k for all $k \geq 1$.

Theorem 2.17. *If $p > 2$, then $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic for all $k \geq 1$.*

Proof. Let g be a primitive root modulo p. If $g^{p-1} \not\equiv 1 \pmod{p^2}$, then we are done by the preceding lemma. Otherwise $g^p \equiv g \pmod{p^2}$. Let $h = (1+p)g$, then h is also a primitive root modulo p since $h \equiv g \pmod{p}$. Also, $h \not\equiv g \pmod{p^2}$ as $p \nmid g$. Hence $h^p = (1+p)^p g^p \equiv g \not\equiv h \pmod{p^2}$ which implies that h generates $(\mathbb{Z}/p^k\mathbb{Z})^\times$ again by the preceding lemma. □

Remark. The proof of Theorem 2.15 fails when $p = 2, k = 1$ since we needed $pk \geq k+2$. Indeed, $(1+2)^2 \equiv 1 \not\equiv 1+4 \pmod{8}$ which is inconsistent with the theorem.
However, it does hold when $p = 2$ and $k \geq 2$ using the same proof. Using this, one can show that $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is generated by -1 (with order 2) and 5 (with order 2^{k-2}) for $k \geq 3$, i.e. $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{k-2}\mathbb{Z})$.

3 Quadratic Residues

3.1 Euler's Criterion and Gauss's Lemma

Definition 3.1. Suppose p is an odd prime and $a \in \mathbb{Z}$ such that $p \nmid a$. We say a is a quadratic residue modulo p if $x^2 \equiv a \pmod{p}$ for some $x \in \mathbb{Z}$. Otherwise, we say that a is a quadratic non-residue modulo p.

In other words, a is a quadratic residue modulo p if and only if its class in $(\mathbb{Z}/p\mathbb{Z})^\times$ is a square.
An open question on this is to give a good estimate of $n(p)$ which is the value of the least quadratic non-residue modulo p. It has been shown that $n(p) \leq cp^\theta$ for some $c > 0$ and any $\theta > \sqrt{e}/4$. Condition on generalised Riemann Hypoethsis, one can show that $n(p) \leq c \log^2 p$ for some $c > 0$.

Example 3.1. Let $p = 7$, then the quadratic residues modulo p are $1, 2, 4$ (and the non-residues are $3, 5, 6$).

Lemma 3.1. *Let p be an odd prime, then there are exactly $(p-1)/2$ qudratic residues modulo p.*

Proof. Consider the map $\sigma : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ that takes x to x^2. σ is two-to-one since $x^2 \equiv y^2 \pmod{p} \iff (x+y)(x-y) \equiv 0 \pmod{p} \implies x \equiv \pm y \pmod{p}$. The number of quadratic residues is just the size of the image of σ which, since σ is two-to-one, is $(p-1)/2$. □

Alternative proof. Take g to be a primitive root modulo p, then the set of quadratic residues is exactly $\{g^{2n} \bmod p : n \in \mathbb{Z}\}$ which has size $(p-1)/2$. □

Definition 3.2. Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0, \text{ if } p \mid a \\ 1, \text{ if } a \text{ is a quadratic residue modulo } p \\ -1, \text{ if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

Theorem 3.2 (Euler's Criterion)**.** *Let p be an odd prime, and $a \in \mathbb{Z}$, then*

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

Remark. Note that if p is an odd prime, then $0, +1, -1$ are distinct, so this congruence determines $\left(\frac{a}{p}\right)$.

Proof. If $p \mid a$ then the result is trivially true.
Suppose henceforth that $p \nmid a$. By Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$ and hence $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. Observe further that if $a \equiv x^2 \pmod{p}$ for some x, then $p \nmid x$ and hence $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$. We know there are exactly $(p-1)/2$ quadratic residues, so the polynomial $a^{(p-1)/2} - 1$ has $(p-1)/2$ roots that happen to the quadratic residues. But it can have at most $(p-1)/2$ roots, hence these are all of them. Euler's criterion follows. □

Corollary 3.3. *Let p be an odd prime and let $a, b \in \mathbb{Z}$, then*

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

Proof. Follows directly from Euler's criterion. □

Remark. This means that $a \mapsto \left(\frac{a}{p}\right)$ is a (surjective) homomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ for odd prime p.
Euler's criterion also tells us that there is a polynomial-time algorithm for computing $\left(\frac{a}{p}\right)$ for odd prime p as there is a polynomial-time algorithm for computing $a^n \bmod p$ for any $n < p-1$:
First, expand n in binary digits $n = n_0 + 2n_1 + \cdots + 2^k n_k$. Then we can compute $a^2 \bmod p, a^4 = (a^2)^2 \bmod p, \ldots, a^{2^k} = (a^{2^{k-1}})^2 \bmod p$ and then use $a^n = \prod_{n_i=1} a^{2^i}$.
In fact, there is a more efficient way to compute $\left(\frac{a}{p}\right)$ which we'll talk about later.

Corollary 3.4. *Let p be an odd prime, then*

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

Proof. Simply plug in Euler's criterion. □

The next question is, when is 2 a quadratic residue modulo p? More generally, is there an easier way to apply Euler's criterion to calculate $\left(\frac{a}{p}\right)$?
By Fermat's little theorem, $a^{p-1} \equiv 1 \pmod p$ for $p \nmid a$. We could, and we did, prove this with Fermat-Euler, but an alternative proof of this would be to observe

$$(p-1)! \equiv \prod_{j=1}^{p-1} j \equiv \prod_{j=1}^{p-1} (aj) = a^{p-1} \prod_{j=1}^{p-1} j \equiv a^{p-1}(p-1)! \pmod p$$

We'll use the same sort of idea. Write $aj = \epsilon_j c_j$ for $c_j \in \{1, 2, \ldots, (p-1)/2\}$ and $\epsilon_j \in \{\pm 1\}$. ϵ_j are certainly uniquely determined. Also, if $c_j = c_k$, then $aj\epsilon_j^{-1} \equiv ak\epsilon_k^{-1} \pmod p$, so $j \equiv \pm k \pmod p$. But $j, k \in \{1, \ldots, (p-1)/2\}$, so $j \equiv k \pmod p$.
Knowing this, it follows that $\{c_1, \ldots . c_{(p-1)/2}\} = \{1, \ldots, (p-1)/2\}$, so

$$a^{(p-1)/2}((p-1)/2)! \equiv \prod_{j=1}^{(p-1)/2} (aj) \equiv \prod_{j=1}^{(p-1)/2} (\epsilon_j c_j) \equiv ((p-1)/2)! \left(\prod_{j=1}^{(p-1)/2} \epsilon_j \right)$$

In other words,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv \prod_{j=1}^{(p-1)/2} \epsilon_j \pmod p$$

We can rephrase this to obtain

Lemma 3.5 (Gauss)**.** *Let p be an odd prime and $a \in \mathbb{Z}$ not divisible by p, then $\left(\frac{a}{p}\right) = (-1)^\mu$ where μ is the number of $j \in \{1, \ldots, (p-1)/2\}$ such that $aj \equiv k \pmod p$ for some $(p+1)/2 \le k \le p-1$*

Example 3.2. (i) Let $a = -1$, then $aj = -j$ for all j, i.e. $\mu = (p-1)/2$. So $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
(ii) Let $a = 2$, then $\{2j : 1 \le j \le (p-1)/2\} = \{2, 4, \ldots, p-3, p-1\}$, so

$\mu = |\{1 \le j \le (p-1)/2 : p/4 < j < p/2\}| = \lfloor p/2 \rfloor - \lfloor p/4 \rfloor$. So the value of $\left(\frac{2}{p}\right)$ depends on p mod 8. More precisely,

$$\left(\frac{2}{p}\right) = \begin{cases} 1, \text{ if } p \equiv \pm 1 \pmod 8 \\ -1, \text{ if } p \equiv \pm 3 \pmod 8 \end{cases}$$

3. Let $a = 3$, then $\mu = |\{1 \le j \le (p-1)/2 : j \in (p/6, p/3)\}| = \lfloor p/3 \rfloor - \lfloor p/6 \rfloor$, so $\left(\frac{3}{p}\right)$ depends on p mod 12.
4. In general, for $1 \le a \le p-1$, we actually have

$$\mu = \sum_{m \in \mathbb{Z}} \left| \left\{ 1 \le j \le \frac{p-1}{2} : \left(m - \frac{1}{2}\right)\frac{p}{a} < j < \frac{mp}{a} \right\} \right|$$

If the m^{th} term is nonzero, then $0 < m < 1/2 + aj/p < (a+1)/2$. In particular, if a is odd, then $1 \le m \le (a-1)/2$.

3.2 Quadratic Reciprocity

Theorem 3.6 (Quadratic Reciprocity)**.** *Let p, q be distinct odd primes, then*

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

This means that $\left(\frac{p}{q}\right)$ is determined by q mod p and p, q mod 4.

Proof. We have $\left(\frac{q}{p}\right) = (-1)^{\mu}$ where $\mu = |\{(j,m) \in S : (m-1/2)p/q < j < mp/q\}|$ and $S = \{(j,m) : 1 \le j \le (p-1)/2, 1 \le m \le (q-1)/2\}$. We can rearrange the expression to obtain $\mu = |\{(j,m) \in S : 0 < mp - jq < p/2\}|$. By symmetry, $\left(\frac{p}{q}\right) = (-1)^{\nu}, \nu = |\{(j,m) \in S : 0 < jq - mp < q/2\}|$. Now

$$|S| = \frac{p-1}{2}\frac{q-1}{2} = \mu + \nu + |A| + |B|$$

where $A = \{(j,m) \in S : mp - jq > p/2\}, B = \{(j,m) \in S : jq - mp > q/2\}$. In fact, $|A| = |B|$ since $(j,m) \mapsto (j', m')$ (where $j' = (p+1)/2 - j, m' = (q+1)/2 - m$) is a one-to-one correspondence between A and B. This means that $\mu + \nu \equiv |S| \equiv (p-1)(q-1)/4 \pmod 2$ which is the result. □

Example 3.3. (i) Let $p \ge 5$ be a prime, then by quadratic reciprocity,

$$\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right) = \begin{cases} 1, \text{ if } p \equiv \pm 1 \pmod{12} \\ -1, \text{ if } p \equiv \pm 5 \pmod{12} \end{cases}$$

(ii) We have

$$\left(\frac{19}{73}\right) = \left(\frac{73}{19}\right) = \left(\frac{16}{19}\right) = 1$$

So 19 is a quadratic residue modulo 73.
(iii)

$$\left(\frac{34}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{17}{97}\right) = \left(\frac{17}{97}\right) = \left(\frac{97}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{2}{17}\right)^2 = \left(\frac{3}{17}\right) = -1$$

by (i).
(iv)

$$\left(\frac{7411}{9283}\right) = -\left(\frac{9283}{7411}\right) = -\left(\frac{1872}{7411}\right) = -\left(\frac{13}{7411}\right) = -\left(\frac{7411}{13}\right) = -\left(\frac{1}{13}\right) = -1$$

Although quadratic reciprocity gives us an algorithm to compute $\left(\frac{p}{q}\right)$ for odd primes p, q, it is quite computationally expensive since we often need to factorise fairly large integers. There is a solution to that, which we shall introduce in a moment.

Definition 3.3. Let $n \geq 1$ be odd and $n = p_1 \cdots p_k$ with p_i not necessarily distinct. We define the Jacobi symbol as

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)$$

with $\left(\frac{a}{1}\right) = 1$ by convention.

Note that $\left(\frac{a}{n}\right) = 0$ if $(a, n) \neq 1$.

Proposition 3.7. *Let $n, m \geq 1$ be odd and $a, b \in \mathbb{Z}$, then:*
(i)

$$a \equiv b \pmod{n} \implies \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$$

(ii)

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right), \left(\frac{a}{mn}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$$

(iii)

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

Proof. (i) and (ii) are obvious; (iii) follows from the identities

$$\frac{x-1}{2} + \frac{y-1}{2} \equiv \frac{xy-1}{2} \pmod{2}, \frac{x^2-1}{8} + \frac{y^2-1}{8} \equiv \frac{(xy)^2-1}{8} \pmod{2}$$

Both of which can be easily verified. □

Theorem 3.8 (Quadratic Reciprocity for Jacobi Symbol)**.** *Let $m, n \geq 1$ be odd, then*

$$\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)$$

Proof. If $(m, n) > 1$ then both sides are zero. Suppose $(m, n) = 1$, we write $m = p_1 \cdots p_k, n = q_1, \ldots, q_l$ with $\{p_i\} \cap \{q_j\} = \varnothing$. Then, using again the fact that $(x-1)/2 + (y-1)/2 \equiv (xy-1)/2 \pmod{2}$,

$$\begin{aligned}
\left(\frac{m}{n}\right) &= \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{p_i}{q_j}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}(-1)^{(p_i-1)(q_j-1)/4}\left(\frac{q_j}{p_i}\right) \\
&= \prod_{i=1}^{k}(-1)^{(p_i-1)(n-1)/4}\prod_{j=1}^{l}\left(\frac{q_j}{p_i}\right) = (-1)^{(m-1)(n-1)/4}\prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{q_j}{p_i}\right) \\
&= (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)
\end{aligned}$$

as desired. □

Remark. How much does the Jacobi symbol modulo n tell us about the squares in $(\mathbb{Z}/n\mathbb{Z})^\times$? Suppose $a \equiv x^2 \pmod{n}$, then $\left(\frac{a}{n}\right) = \left(\frac{x}{n}\right)^2 = 1$, so squares in $(\mathbb{Z}/n\mathbb{Z})^\times$ has Jacobi symbol 1. However, the converse is not true: $\left(\frac{2}{15}\right) = 1$ but 2 is not a square modulo 15.
More generally, let $p \neq q$ be distinct odd primes and $a \in \mathbb{Z}$ has $(a, pq) = 1$, then the Chinese Remainder Theorem implies that a is square moduulo pq iff a is a square modulo p and modulo q. The Jacobi symbol messes up this information when a is a quadratic non-residue modulo both p and q. In general, it can only tell the parity of the number of times when a fails to be a square modulo a prime factor of n.

The virtue of Jacobi symbol is the assistant it offers to compute the Legendre symbol: We no longer need to factorise many times since quadratic reciprocity holds for Jacobi symbols – all we need to do are divisions by 2.

Example 3.4. 1.

$$\left(\frac{33}{73}\right) = \left(\frac{73}{33}\right) = \left(\frac{7}{33}\right) = \left(\frac{33}{7}\right) = \left(\frac{5}{7}\right) = -1$$

2.

$$\left(\frac{66}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{33}{73}\right) = \left(\frac{33}{73}\right) = -1$$

Or, alternatively,

$$\left(\frac{66}{73}\right) = \left(\frac{-7}{73}\right) = \left(\frac{-1}{73}\right)\left(\frac{7}{73}\right) = \left(\frac{7}{73}\right) = \left(\frac{73}{7}\right) = \left(\frac{3}{7}\right) = -1$$

Remark. 1. What about higher powers? It is easy to check that if $p \equiv 2 \pmod{3}$, then every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cube. However, if $p \equiv 1 \pmod{3}$, then one can define a cubic residue symbol taking values in $\{0, 1, e^{2\pi i/3}, e^{4\pi i/3}\}$ analogously.
2. When p is odd, $\left(\frac{-1}{p}\right) = 1$ iff $p \equiv 1 \pmod{4}$. But this happens iff $p = x^2 + y^2 = (x + iy)(x - iy)$ for some x, y (as we will see later). The ultimate generalisations of these kind of statements is known as Artin's reciprocity law, which describes how primes in factor in certain number rings.

4 Binary Quadratic Forms

4.1 Equivalence and Discriminants

Which integers can be represented as the sum of two integer squares?

Theorem 4.1. *Let $N \in \mathbb{N}$, then N is the sum of two squares if and only if every prime $p \equiv 3 \pmod{4}$ dividing N divides N to an even power.*

Proof. If $N = x^2 + y^2$ and $p \equiv 3 \pmod{4}$ is a prime that divides N, then $x^2 = -y^2 \pmod{p} \implies x \equiv y \equiv 0 \pmod{p}$ as $\left(\frac{-1}{p}\right) = -1$, so $p^2 \nmid N$. One can repeat this process for $N/p^2 = (x/p)^2 + (y/p)^2$ to conclude that p divides N to an even power.

Conversely, write $N = M^2K$ where K is the product if distinct primes that's either 2 or is congruent to 1 modulo 4. It suffices to show $K = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. The identity $(x^2 + y^2)(w^2 + z^2) = (xw + yz)^2 + (xz - yw)^2$ reduces the problem to writing a prime p congruent to 1 modulo 4 as the sum of two squares.
We will complete the rest of the proof later, after we have established enough theory. □

Definition 4.1. A binary quadratic form with integer coefficients (BQF) is a polynomial $f(x, y) = ax^2 + bxy + cy^2$ for some $a, b, c \in \mathbb{Z}$. We say f represents $n \in \mathbb{Z}$ if n is in the image of f.

We sometimes write (a, b, c) in place of f. It is also helpful to regard f in the form

$$f(x, y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Example 4.1. 1. $f(x, y) = x^2 + y^2$, or $(1, 0, 1)$, has matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.
2. $g(x, y) = 4x^2 + 12xy + 10y^2$, or $(4, 12, 10)$, has matrix $\left(\begin{smallmatrix} 4 & 6 \\ 6 & 10 \end{smallmatrix}\right)$. Note that $g(x, y) = (2x + 3y)^2 + y^2 = f(2x + 3y, y)$, so we can regard f, g as related by a change of variable $g(x, y) = f(X, Y)$ with

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

However, f, g do not represent the same integers since f represents 1 but g does not. To make sense of it, one might need to observe that the inverse of $\left(\begin{smallmatrix} 2 & 3 \\ 0 & 1 \end{smallmatrix}\right)$ does not have integer coefficients.

Definition 4.2. A unimodular substitution is a change of variables in the form $(X, Y) = (x, y)A$ with $A \in \mathrm{SL}_2(\mathbb{Z})$.
Two BQFs f and g are said to be equivalent if $f(X, Y) = g(x, y)$ for one such unimodular substitution $(x, y) \mapsto (X, Y)$.

Remark. 1. Since $\mathrm{SL}_2(\mathbb{Z})$ is a group, the equivalence of BQFs is indeed a equivalence relation.
2. Equivalent forms represent the same integers.

Example 4.2. $(4, 12, 10)$ is not equivalent to $(1, 0, 1)$, but it is equivalent to $(2, 0, 2)$ via $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right)$.

From an algebraic viewpoint, we can let $\mathrm{SL}_2(\mathbb{Z})$ act on the set of (matrices of) BQFs via the change of variable. Say $g(x, y) = f(X, Y)$ where $(X, Y) = (x, y)A$ for some $A \in \mathrm{SL}_2(\mathbb{Z})$, then we simply have $M_g = AM_fA^\top$ where M_g, M_f are understood to be the respective matrices of f, g. Consequently, this is a well-defined group action whose orbit is the equivalence classes of BQFs.

Definition 4.3. Let $f = (a, b, c)$ be a BQF, then its discriminant is $\mathrm{disc}(f) = b^2 - 4ac = -4 \det M_f$.

Example 4.3. 1. $\mathrm{disc}(1, 0, 1) = -4, \mathrm{disc}(4, 12, 10) = -16$.

Lemma 4.2. *Equivalent BQFs have the same discriminant.*

Proof. $\mathrm{disc}(f) = -4 \det M_f$. □

However, BQFs can have the same discriminant but not equivalent. For example, x^2+6y^2 and $2x^2+3y^2$ both have discriminant -24 but 1 is represented by the former but not the latter.

Lemma 4.3. *There exists a BQF f with discriminant d if and only if $d \equiv 0, 1 \pmod 4$.*

Proof. If $d = \mathrm{disc}(f) = b^2 - 4ac$ for some $a, b, c \in \mathbb{Z}$, then $d \equiv b^2 \equiv 0, 1 \pmod 4$. Conversely, if $d \equiv 0 \pmod 4$ then we can take $f = (1, 0, -d/4)$ and if $d \equiv 1 \pmod 4$ then we can take $f = (1, 1, (1-d)/4)$. □

Note that any BQF is in particular a real quadratic form.

Definition 4.4. A real quadratic form $f(x_1, \ldots, x_n) = \sum_{i \le j} a_{ij} x_i x_j$ with $a_{ij} \in \mathbb{R}$ is said to be:
1. Positive definite if $f(\underline{x}) > 0$ for all $\underline{x} \in \mathbb{R}^n - \{0\}$.
2. Negative definite if $f(\underline{x}) < 0$ for all $\underline{x} \in \mathbb{R}^n - \{0\}$.
3. Indefinite if there are $\underline{x}, \underline{y} \in \mathbb{R}^n$ with $f(\underline{x}) > 0 > f(\underline{y})$.

Lemma 4.4. *Let $f = (a, b, c)$ be a BQF and let $d = \mathrm{disc}(f)$. Then:*
(i) If $d < 0, a > 0$, then f is positive definite.
(ii) If $d < 0, a < 0$, then f is negative definite.
(iii) If $d > 0$, then f is indefinite.
(iv) If $d = 0$, then $f = l(mx + ny)^2$ for some $l, m, n \in \mathbb{Z}$.

Proof. (i) and (ii) follow from the fact that $4af(x, y) = 4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 + (4ac - b^2)y^2 = (2ax + by)^2 - dy^2 > 0$ for all x, y since $d < 0$.
For (iii), if $a = c = 0$, then $f(1, -1)$ and $f(1, 1)$ have distinct signs, i.e. f is indefinite. Otherwise WLOG $a \neq 0$, then $f(-b, 2a)$ and $f(1, 0)$ are both nonzero and have distinct signs since $d > 0$, which means that f is indefinite.
For (iv), write $a = a_1 a_2^2$ with a_1 a product of distinct primes. Then if $b^2 = 4ac$ then $2a_1a_2 \mid b$, hence

$$ax^2 + bxy + cy^2 = a_1 \left(a_2 x + \frac{b}{2a_1 a_2} y \right)^2$$

which has the desired form. □

Remark. 1. There are indefinite forms with positive coefficients: $\mathrm{disc}(1, 3, 1) = 5 > 0$.
2. There are positive definite forms with some of whose coefficients nonpositive: $\mathrm{disc}(1, -1, 2) = -7 < 0$.
3. However, if $d < 0$ and $a > 0$, then necessarily $c > 0$.

Our focus now is on positive definite BQFs. Specifically, we want to find the "simplest" expression of a representative of an equivalence class of positive definite BQFs.

4.2 Reduced Positive Definite BQFs

If $f(x, y) = ax^2 + bxy + cy^2$, then the substitution $(X, Y) = (x, y) \left(\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right)$ yields $f(X, Y) = ax^2 + (b + 2\lambda a)xy + (\lambda^2 a + \lambda b + c)y^2$. Taking $\lambda = \pm 1$ shows that (a, b, c) is equivalent to $(a, b \pm 2a, a \pm b + c)$.

Example 4.4. By repeatly using the transformation we obtain the equivalence of $(10, 34, 29)$ and $(10, -6, 1)$.

How would we reduce the size of a? Consider the substitution $(X, Y) = (x, y)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ which gives $f(X, Y) = ay^2 - bxy + cx^2$. That is, (a, b, c) is equivalent to $(c, -b, a)$.

Example 4.5. $(10, 34, 29)$ is equivalent to $(10, -6, 1)$, which is equivalent to $(1, 6, 10)$ by this new operation. Using the first operation again (and again) gives the equivalence of $(10, 34, 29)$ and $(1, 0, 1)$.

To summarise, we know that one can replace f by an equivalent form with the same coefficient a but $|b| \leq a$ by applying the first operation repeatedly. By applying the second, one can replace f by an equivalent form with $a \leq c$ and $|b|$ unchanged.

Definition 4.5. A positive definite BQF is said to be reduced if either $-a < b \leq a < c$ or $0 \leq b \leq a = c$.

Example 4.6. $(10, 34, 29)$ is not reduced but $(1, 0, 1)$ is.

Proposition 4.5. *Every positive definite BQF is equivalent to a reduced form.*

Proof. Call the operations $T_\pm : (a, b, c) \mapsto (a, b \pm 2a, a \pm b + c), S : (a, b, c) \mapsto (c, -b, a)$. If $a > c$, use S to decrease a while keeping $|b|$ unchanged; If $a \leq c$ and $|b| > a$, use $T_\pm$ to decrease $|b|$ while maintaining a unchanged. Repeatedly applications of S and $T_\pm$ in this way must terminate since $a + |b|$ is decreased in each step.
At the end we arrive at a form (a, b, c) with $a \leq c$ and $|b| \leq a$. If $a < c$, then either $b > -a$ in which case the form is already reduced, or $b = -a$, in which case T_+ takes it to (a, a, c) which is reduced. If $a = c$, then either (a, b, c) is reduced or $-a \leq b < 0$. For the latter case, S takes it to $(a, -b, a)$ which is reduced. □

Lemma 4.6. *Suppose $f = (a, b, c)$ is a reduced positive definite BQF with discriminant d, then $|b| \leq a \leq \sqrt{|d|/3}$ and $b \equiv d \pmod 2$.*

Proof. $d = \operatorname{disc}(f) = b^2 - 4ac \equiv b^2 \equiv b \pmod 2$.
As for the inequality, since f is reduced, $|b| \leq a \leq c$, so $d = b^2 - 4ac \leq ac - 4ac = -3ac \leq -3a^2 \implies a^2 \leq |d|/3$. □

Example 4.7. Suppose $f = (a, b, c)$ is a reduced positive definite BQF with $\operatorname{disc}(f) = -4$, then $a^2 \leq 4/3$, so $a = 1, |b| \leq 1$, therefore $b = 0$ since we also need $b \equiv d \pmod 2$, i.e. $f = (1, 0, 1)$. In other words, $f = (1, 0, 1)$ is the only reduced positive definite BQF of discriminant -4, and hence any other positive definite BQF must be equivalent to it.

Proof of Theorem 4.1 (cont.) What we left off was to show that any prime p that is congruent to 1 modulo 4 is a sum of two squares. As $\left(\frac{-1}{p}\right) = 1$, there are $m, k \in \mathbb{Z}$ such that $m^2 = -1 + kp$. Let $f = (p, 2m, k)$, then $f(1, 0) = p$ and $\operatorname{disc}(f) = (2m)^2 - 4pk = -4$, so f is equivalent to $(1, 0, 1)$, which means that $x^2 + y^2$ represents p, i.e. p is the sum of two squares. □

Definition 4.6. We say a BQF f properly represents $n \in \mathbb{Z}$ if there is $x, y \in \mathbb{Z}$ such that $(x, y) = 1$ and $n = f(x, y)$.

Remark. Note that if we have a change of variable $(X, Y) = (x, y)A$ for $A \in \mathrm{SL}_2(\mathbb{Z})$, then $d \mid (x, y)$ iff $d \mid (X, Y)$. Hence equivalent forms do not just represent the same integers, they actually properly represent the same integers.

Lemma 4.7. *The least integers properly represented by a reduced positive definite BQF $f = (a, b, c)$ are $a, c, a - |b| + c$, in this order.*

Remark. By convention, values in the (ascending) list of integers properly represented by f are repeated k times if there are k different proper representation of it, discounting the obvious repeats $f(x, y) = f(-x, -y)$.

Proof. If $f(x, y) = n$ properly, then $(x, y) = 1$, in particular x, y are not both zero. If $f(x, 0) = n$ properly, then $x = \pm 1$ and $n = f(\pm 1, 0) = a$; If $f(0, y) = n$ properly, then $y = \pm 1$ and $n = f(0, \pm 1) = c \geq a$. Suppose now that $|x| \geq |y| > 0$, then

$$f(x, y) = ax^2 + bxy + cy^2 \geq ax^2 - |b||x||y| + cy^2 \geq (a - |b|)x^2 + cy^2 \geq a - |b| + c \geq c$$

Similarly, $|y| \geq |x| > 0$ also gives $f(x, y) \geq a - |b| + c \geq c$. In addition, $f(1, -\operatorname{sgn}(b)) = a - |b| + c$. This concludes the proof. □

Theorem 4.8. *Every positive definite BQF is equivalent to a unique reduced form.*

Proof. We already know that every positive definite BQF is equivelent to at least one reduced form. Thus it suffices to show that equivalent reduced positive definite BQFs have to equal. Suppose (a, b, c) and (a', b', c') are equivalent reduced positive definite BQFs. We know that $a = a', c = c', b' = \pm b$ by the preceding lemma.
If $b = 0$, then $f = g$. If $b > 0$, (a, b, c) and $(a, -b, c)$ cannot both be reduced: Suppose they were, then $a < c$ and $|b| < a$. Consequently, the smallest values properly represented by f, g are $a < c < a - |b| + c$ without repeats. This means that if $f(X, Y) = g(x, y)$, then $(X, Y) = (\pm 1, 0) \iff (x, y) = (\pm 1, 0)$ and $(X, Y) = (0, \pm 1) \iff (x, y) = (0, \pm 1)$, which means that the change-of-variable matrix is $\pm I$, i.e. $f = g$. □

Definition 4.7. Let $d > 0, d \equiv 0, 1 \pmod 4$. The class number $h(d)$ is the number of reduced positive definite BQFs of discriminant d.

Equivalently, $h(d)$ is the number of equivalence classes of positive definite BQFs of discriminant d.

Example 4.8. We have seen that there is only one reduced positive definite BQF with discriminant -4, i.e. $h(-4) = 1$.
Consider $d = -24$, then the forms $x^2 + 6y^2$ and $2x^2 + 3y^2$ have discriminant -24. Are there any others? Suppose (a, b, c) has determinant -24. By Lemma 4.6, we have $|b| \leq a \leq \sqrt{24/3} = 2\sqrt{2} \implies |b| \leq a \leq 2$ and $b \equiv d \pmod 2$. If $a = 1$, then $b = 0$ and $c = (b^2 - d)/(4a) = 6$. If $a = 2$, then $b \in \{0, \pm 2\}$, but $((\pm 2)^2 + 24)/8 \notin \mathbb{Z}$, so $b = 0$ and hence $c = 3$.
So indeed $h(-24) = 2$.

A natural question to ask is how does h behaves as a function of d. Heilbronn (1944) showed that $h(d) \to \infty$ as $d \to \infty$. Also, Mertens (1874) has shown that

$$\frac{1}{N} \sum_{3 \leq -d \leq N} h(d) \sim \frac{\pi}{18} \sqrt{N}$$

It turns out that we can characterise (Baker-Stark, 1967) all discriminants d such that $h(d) = 1$: They are $-3, -4, -7, -8, -11, -19, -43, -67, -163$ and $-12, -16, -27, -28$ (the first group collects those discriminants in this list that are fundamental, a concept we shall cover later). In general, given $h \geq 1$, there is an explicit bound on the number of d such that $h(d) = h$. So in principle we can compute all discriminants that satisfies $h(d) = h$. However, the bound is in general quite large, so one often use other methods in practice.

4.3 More on Proper Representations

Lemma 4.9. *Let $n \in \mathbb{N}$ and let f be a BQF, then f properly represents n iff f is equivalent to (n, b, c) for some b, c.*

Proof. The "if" direction is obvious. Conversely, if $f(\alpha, \beta) = n$ for some $\alpha, \beta \in \mathbb{Z}, (\alpha, \beta) = 1$, then pick $\gamma, \delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1$. Hence f is equivalent to $g(x, y) = f(\alpha x + \gamma y, \beta x + \delta y)$ whose x^2 coefficient is n, as desired. □

Theorem 4.10. *Let $n \in \mathbb{N}$ and $d < 0$ with $d \equiv 0, 1 \pmod 4$, then n is properly represented by some BQF of discriminant d if and only if $x^2 \equiv d \pmod{4n}$ is soluble.*

Proof. If n is properly represented by f and $\operatorname{disc}(f) = d$, then the preceding lemma implies that f is equivalent to (n, b, c) for some $b, c \in \mathbb{Z}$. In particular, $b^2 - 4nc = d \implies b^2 \equiv d \pmod{4n}$.
Conversely, suppose there is some integer b such that $b^2 \equiv d \pmod{4n}$, then there is some $c \in \mathbb{Z}$ such that $b^2 = d + 4nc$, hence (n, b, c) has discriminant d and properly represents n. □

We want to know which integers can be properly represented by $f(x, y) = x^2 + xy + 2y^2$. $\operatorname{disc}(f) = -7 < 0$ and f is in fact a (reduced) positive definite BQF. We claim $h(-7) = 1$. Indeed, if (a, b, c) is reduced and has discriminant -7, then $|b| \leq a \leq \sqrt{7/3}$ and $b \equiv d \pmod 2$, so $|b| \leq a \leq 1$ and b is odd, thus $a = |b| = 1$. So $c = (b^2 - d)/4a = 2$. But then $(a, b, c) = (1, 1, 2)$ since $(1, -1, 2)$ is not reduced. Consequently, f properly represents n iff $x^2 \equiv -7 \pmod{4n}$ for some $x \in \mathbb{Z}$ by the preceding theorem.
Case 1: $n = p$ is prime. If $p = 2, 7$, we observe that $f(0, 1) = 2, f(1, -2) = 7$, so f properly represents $2, 7$. Assume henceforth that $p \neq 2, 7$. $x^2 \equiv -7 \pmod{4p}$ is soluble iff -7 is a square modulo both 4 and p. -7 is certainly a square modulo 4, also

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

by quadratic reciprocity. In conclusion, f properly represents a prime p iff $p = 0, 1, 2, 4 \pmod 7$.
Case 2: n is composite. Let $n = \prod_p p^{\alpha_p}$ be the decomposition of n into powers of distinct primes. Then $x^2 \equiv -7 \pmod{4n}$ is soluble iff -7 is a square modulo $2^{2+\alpha_2}$ and p^{α_p} for all odd $p \mid n$.

Lemma 4.11. *Suppose $a \in \mathbb{Z}$, then:*
(i) If $a \equiv 1 \pmod 8$, then a is a square modulo 2^k for all $k \geq 1$.
(ii) If $p > 2$ is prime and $\left(\frac{a}{p}\right) = 1$, then a is a square modulo p^k for all $k \geq 1$.

Proof. (i) We proceed by induction on k. It is clear for $k \leq 3$. Suppose henceforth that $\exists x \in \mathbb{Z}$ such that $x^2 = a + 2^k m$ for some $m \in \mathbb{Z}$ and $k \geq 3$. If m is even, then $x^2 \equiv a \pmod{2^{k+1}}$. If m is odd, then $(x + 2^{k-1})^2 = x^2 + 2^k x + 2^{2k-2} = a + 2^k(x + m) + 2^{2k-2} \equiv a \pmod{2^{k+1}}$. In both cases, we have shown that a is a square modulo 2^{k+1}, which completes the induction.
(ii) Again induction on k. Since $\left(\frac{a}{p}\right) = 1$, there is some x such that $x^2 \equiv a \pmod p$. Suppose there is some $x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod{p^k}$ for some $k \geq 1$, i.e. $x^2 = a + mp^k$ for some $m \in \mathbb{Z}$. For $t \in \mathbb{Z}$, consider $(x + p^k t)^2 \equiv x^2 + 2p^k tx \equiv a + (m + 2tx)p^k \pmod{p^{k+1}}$. Choosing t such that $p \nmid (2tx + m)$, which is possible since $(2x, p) = 1$, demonstrates that a is a square modulo p^{k+1}. This completes the induction and the proof. □

The first part of the lemma tells us that -7 is always a square modulo $2^{2+\alpha_2}$. The second part of the lemma tells us that if $p \neq 7$ is prime, then -7 is a square modulo p^k if and only if $\left(\frac{-7}{p}\right) = 1$, or $p \equiv 1, 2, 4 \pmod 7$. If $p = 7$, then $x^2 \equiv -7 \pmod{7^k}$ is soluble for $k \leq 1$, but not if $k \geq 2$.
In conclusion, $f = (1, 1, 2)$ properly represents n if and only if the prime decomposition of n is $n = 7^{\alpha_7} \prod_{p \equiv 1,2,4 \pmod 7} p^{\alpha_p}$ with $\alpha_7 \leq 1$.
But when does f (not necessarily properly) represent an integer n? We can always scale stuff, so they are all integers of the form $k^2 n$ with $k \geq 0$ and n properly represented by n. Consequently, $n = x^2 + xy + y^2$ if and only if every prime $p \equiv 3, 5, 6 \pmod 7$ divides n to an even power.

Remark. 1. If $h(d) = 1$, an analogue of the above procedure implies that we have completely solved (in principle) the problem of which integers are represented by a given BQF of discriminant $d < 0$. If $h(d) > 1$, we can determine which integers are represented by some form of discriminant d, but no better. For some values of d, we can make use of additional congruence relations to distinguish exactly which BQFs of discriminant d represent a certain number. This sometimes fails, e.g. when we try to solve $p = x^2 + 23y^2$.
2. An integer $d \equiv 0, 1 \pmod 4$ is said to be a fundamental discriminant if it is not of the form $d = k^2 d'$ with $k > 1$ and $d' \equiv 0, 1 \pmod 4$. For a fundamental discriminant $d < 0$, Gauss defined a law of composition which makes the set of equivalence classes of BQFs of discriminant d into an abelian group. This turns out to be the ideal class group of the number field $\mathbb{Q}(\sqrt{d})$.
3. What about indefinite forms? If f is positive definite, then there are only a finite number of representations of n by f since the equation $f(x, y) \leq n$ is a bounded region in $\mathbb{R}^2$ (which can only contain a finite number of lattice point of $\mathbb{Z}^2$). However, if f is indefinite, there can be infinitely many such representations. For example, $1 = x^2 - 2y^2$ has solutions $(1, 0)$ and $(3, 2)$, but if (x, y) is a solution, so is $(x^2 + 2y^2, 2xy)$ – hence there are infinitely many solutions.

What about integer quadratic forms in more than two variables? It's a result of Lagrange (1770) that every positive integer is a sum of four squares. Legendre (1797) showed that a positive integer n is a sum of three squares iff $n \neq 4^a(8b + 7)$ for some $a, b \geq 0$.

Waring's problem (1770) enquires the properties of $g(k)$ which is the least positive integer s such that every integer can be represented by a sum of s k^{th} powers. Finiteness of $g(k)$ for all k was proved by Hilbert (1909), and we know that $g(2) = 4, g(3) = 9, g(4) = 19$, but the asymptotic growth of g remains an active area of research.

5 Distribution of Primes

The sequence of primes $2, 3, 5, 7, \ldots$ is always an interesting mathematical object. One can ask many problems about this sequence. How rapidly does it grow? How regular is this sequence?

5.1 The Fancy Theorems

The first question is answered by a result known as the prime number theorem.

Theorem 5.1 (Prime Number Theorem)**.** *Let $\pi(x)$ be the number of primes at most x, then $\pi(x) \sim x/\log x$ as $x \to \infty$.*

Remark. In case you forgot, the big-O and little-o notation means the following: Given two functions $f, g : \mathbb{R}_{>0} \to \mathbb{R}$, we write $f = O(g)$ as $x \to \infty$ if there is some $C > 0$ and $x_0 \in \mathbb{R}_{>0}$ such that $|f(x)| < C|g(x)|$ for any $x \geq x_0$. For example, $2x^3 - 4x^2 + x = O(x^3), x(\log x)^2 = O(x^2)$ as $x \to \infty$.
We write $f = o(g)$ as $x \to \infty$ if $\forall \epsilon > 0, \exists x_0 \in \mathbb{R}_{>0}$ such that $|f(x)| < \epsilon |g(x)|$ for all $x \geq x_0$. For example, $x(\log x)^{-2} = o(x/\log x)$ and $x(\log x)^2 = o(x^2)$ as $x \to \infty$. If g is eventually nonvanishing, then $f = o(g)$ as $x \to \infty$ is equivalent to say $f/g \to 0$ as $x \to \infty$. In particular, $f = o(1)$ as $x \to \infty$ is to say $f(x) \to 0$ as $x \to \infty$.
We write $f \sim g$ as $x \to \infty$ if $f = (1 + o(1))g$ as $x \to \infty$.

There are other ways to state the prime number theorem, for example we can say that $\pi(x) \sim \mathrm{Li}(x)$ where

$$\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\log t}$$

is the logarithmic integral.
We can make this stronger by adding in an estimate for the error term

Theorem 5.2. *There is a constant $C > 0$ such that*

$$\pi(x) = \frac{x}{\log x} + O(x \exp(-C\sqrt{\log x}))$$

Another kind of flavour these prime-distribution results come in as are those about the position of primes in arithmetic progressions. We have seen in IA Numbers & Sets that there are infinitely many primes congruent to $1, 3$ modulo 4. There are even stronger results about phenomena like this.

Theorem 5.3 (Dirichlet)**.** *Let a, q be positive coprime integers, then there are infinitely many primes congruent to a modulo q.*

Theorem 5.4 (Siegel-Walfisz)**.** *Let $a, q \in \mathbb{Z}, (a,q) = 1$ and let $\pi(x;q,a)$ be the number of primes $p \le x$ such that $p \equiv a \pmod q$. For all real $B > 0$, there is some $C_B > 0$ such that*

$$\pi(x;q,a) = \frac{x}{\varphi(q)\log x} + O(x\exp(-C_B\sqrt{\log x}))$$

whenever $q \le (\log x)^B$.

We are not gonna prove all these theorems, but we shall introduce the protagonist of the proof, namely the Riemann ζ function. We will also prove Tchebychev's theorem: There is some $c_2 > c_1 > 0$ such that for any $x > 1$,

$$c_1\frac{x}{\log x} \le \pi(x) \le c_2\frac{x}{\log x}$$

We are not gonna get there anytime soon, so let's have a little treat first.

5.2 Elementary Bounds

Lemma 5.5. *Let $x \in \mathbb{N}$, then $\pi(x) \ge \log x/(2\log 2)$*

Proof. Let $p_1, \dots, p_r$ be primes up to x, so $r = \pi(x)$. Every $n \le x$ can be written as $n = k^2\prod_{i=1}^r p_i^{\alpha_i}$ with $\alpha_i \in \{0,1\}$ and $1 \le k \le \sqrt{x}$. There are at most 2^r choices of these α_i and at most $\sqrt{x}$ choice of k, so $x \le \sqrt{x}2^r = \sqrt{x}2^{\pi(x)}$ which implies the result. □

Theorem 5.6. *(i) For $x \ge 5$, we have $\sum_{p\ prime \le x} p^{-1} \ge \log\log x - 1/2$, in particular $\sum_{p\ prime} p^{-1}$ diverges.*
(ii) For $x \ge 2$, $\prod_{p\ prime \le x}(1-p^{-1})^{-1} \ge \log x$, in particular $\prod_p (1-p^{-1})^{-1}$ diverges.

Remark. In fact, it can be shown that there is a constant c such that

$$\sum_{p\ \text{prime} \le x} \frac{1}{p} = \log\log x + c + O\left(\frac{1}{\log x}\right)$$

and also

$$\prod_{p\ \text{prime} \le x}\left(1-\frac{1}{p}\right)^{-1} = e^\gamma \log x + O(1)$$

where $\gamma \approx 0.5772$ is Euler–Mascheroni constant.

Proof. Let's prove (ii) first. We have

$$\begin{aligned}\prod_{p\ \text{prime} \le x}\left(1-\frac{1}{p}\right)^{-1} &= \prod_{p\ \text{prime} \le x}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)\\ &\ge \sum_{n \le x}\frac{1}{n} \ge \int_1^{x+1}\frac{\mathrm{d}y}{y} \ge \log x\end{aligned}$$

As for (i), we estimate

$$\begin{aligned}
&\log\left(\prod_{p \text{ prime}\le x}\left(1-\frac{1}{p}\right)^{-1}\right)-\sum_{p \text{ prime}\le x}\frac{1}{p}=\sum_{p \text{ prime}\le x}\left(-\log\left(1-\frac{1}{p}\right)-\frac{1}{p}\right)\\
&=\sum_{p \text{ prime}\le x}\left(\frac{1}{2p^2}+\frac{1}{3p^3}+\frac{1}{4p^4}+\cdots\right)\le\sum_{p \text{ prime}\le x}\frac{1}{2p^2}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)\\
&=\sum_{p \text{ prime}\le x}\frac{1}{2p^2}\frac{1}{1-p^{-1}}=\sum_{p \text{ prime}\le x}\frac{1}{2p(p-1)}\le\sum_{2\le n\le x}\frac{1}{2n(n-1)}\\
&=\frac{1}{2}\sum_{2\le n\le x}\left(\frac{1}{n-1}-\frac{1}{n}\right)=\frac{1}{2}\left(1-\frac{1}{x}\right)\le\frac{1}{2}
\end{aligned}$$

which gives the result by (ii). □

Turns out, the values we considered here are closely related to the Riemann ζ function.

5.3 The Riemann ζ Function

Definition 5.1. For a complex number s with $\operatorname{Re} s > 1$, we define

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$$

This is known as the Riemann ζ function.

Conventionally, we write $s=\sigma+it$.

Lemma 5.7. *For* $\operatorname{Re}(s) > 1$*, then series defining* $\zeta(s)$ *converges absolutely. Moreover, it converges uniformly on* $\{\operatorname{Re}(s) \ge 1+\delta\}$ *for any* $\delta > 0$*, thus is analytic on* $\operatorname{Re}(s) > 1$*.*

Proof. Writing $|n^s| = n^\sigma$ gives absolute convergence. Combining this with Weierstrass' M-test then gives the uniform convergence. □

Theorem 5.8. *For* $s \in \mathbb{C}$ *with* $\operatorname{Re}(s) > 1$*, we have*

$$\zeta(s)=\prod_{p \text{ prime}}\left(1-\frac{1}{p^s}\right)^{-1}$$

Remark. (i) The right-hand side is known as the Euler product for ζ.
(ii) In particular, for $\operatorname{Re}(s) > 1$ we have

$$\prod_{p \text{ prime}\le x}\left(1-\frac{1}{p^s}\right)^{-1}\to\zeta(s)$$

as $x \to \infty$.

Sketch of proof.

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p \text{ prime}} (1 + p^{-s} + p^{-2s} + \cdots) = \sum_{n \geq 1} n^{-s}$$

since every n^{-s} occurs exactly once in the supposedly-expanded expression. □

Proof. Let $s = \sigma + it$ for $\sigma > 1$ and consider

$$\begin{aligned} \zeta(s) - \prod_{p \text{ prime} \leq x} \left(1 - \frac{1}{p^s}\right)^{-1} &= \sum_{n \geq 1} n^{-s} - \prod_{p \text{ prime} \leq x} (1 + p^{-s} + p^{-2s} + \cdots) \\ &= \sum_{n \in \mathbb{N}_x} n^{-s} \end{aligned}$$

where $\mathbb{N}_x$ collects all natural numbers at least one of whose prime factors is strictly greater than x. Hence

$$\left| \zeta(s) - \prod_{p \text{ prime} \leq x} \left(1 - \frac{1}{p^s}\right)^{-1} \right| \leq \sum_{n \in \mathbb{N}_x} n^{-\sigma} \leq \sum_{n > x} n^{-\sigma} \to 0$$

as $x \to \infty$. □

Corollary 5.9. $\zeta(s) \neq 0$ *whenever* $\mathrm{Re}(s) > 1$.

Proof. Clearly $\prod_{p \text{ prime} \leq x} (1 - p^{-s})^{-1} \neq 0$ for any $x \geq 2$. Note that

$$\zeta(s) \prod_{p \text{ prime} \leq x} (1 - p^{-s}) = \prod_{p > x} (1 - p^{-s})^{-1} = 1 + \sum_{n \in \mathbb{N}'_x} n^{-s}$$

where $\mathbb{N}'_x$ collects all natural numbers all of whose prime factors are strictly greater than x. Hence

$$\left| \zeta(s) \prod_{p \text{ prime} \leq x} (1 - p^{-s}) \right| \geq 1 - \sum_{n > x} n^{-\sigma} \to 1$$

as $x \to \infty$. In particular $\zeta(s)$ cannot be zero. □

Remark. It turns out we can extend ζ meromorphically to the whole of $\mathbb{C}$. Consider the Γ function defined by

$$\Gamma(z) = \int_0^\infty e^{-t} t^{z-1} \, \mathrm{d}t$$

for $\mathrm{Re}(z) > 0$. This can be continued meromorphically to $\mathbb{C}$ with simple poles at $z = 0, -1, -2, \ldots$. It also satisfies $z\Gamma(z) = \Gamma(z + 1)$ globally (and therefore has $\Gamma(n) = (n - 1)!$).
One then defines the completed ζ function $\Xi(s) = \pi^{s/2}\Gamma(s/2)\zeta(s)$ which satisfies the functional equation $\Xi(s) = \Xi(1 - s)$. This allows us to extend Ξ and hence ζ to the whole of $\mathbb{C}$. Turns out ζ has only one simple pole at $s = 1$ with residue 1 and has trivial zeros at $s = -2, -4, -6, \ldots$. Since ζ is nonvanishing for $\mathrm{Re}(s) > 1$, then functional equation tells us that any further zeros of ζ lie in the critical strip $0 \leq \mathrm{Re}(s) \leq 1$. The nonvanishing of ζ on the line $\mathrm{Re}(s) = 1$ would imply the prime number theorem. The Riemann hypothesis asserts that, in fact, all zeros of ζ lie on the line $\mathrm{Re}(s) = 1/2$.

Definition 5.2. The Möbius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$ by $\mu(1) = 1$ and

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes} \\ 0 & \text{if } n \text{ is not square-free} \end{cases}$$

On the example sheet, you will show that μ is a multiplicative function. You will also show the Möbius inversion formula

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

using the following lemma:

Lemma 5.10. $\nu(n) = \sum_{d|n} \mu(d) = 1_{n=1}$.

Proof. ν is multiplicative since μ is. We also know $\nu(1) = 1$ and $\nu(p^a) = 0$ for $a \geq 1$, hence the lemma. □

Remark. It is known that the Riemann Hypothesis is equivalent to the assertion that for any $\epsilon > 0$, there is $C_\epsilon > 0$ such that $|\sum_{n \leq x} \mu(n)| \leq C_\epsilon x^{1/2+\epsilon}$.

Definition 5.3. A Dirichlet series is an infinite series of the form $\sum_{n \geq 1} a_n n^{-s}$ for some sequence $a_n \in \mathbb{C}$.

Remark. If $|a_n|$ is bounded by Cn^k for some $k > 0$, then the said Dirichlet series converges absolutely on $\mathrm{Re}(s) > k + 1$ and uniformly on $\mathrm{Re}(s) \geq k + 1 + \delta$ for any $\delta > 0$.

Example 5.1. (i) ζ is a Dirichlet series.
(ii)

$$\sum_{n=1}^{\infty} \left(\frac{n}{p}\right) \frac{1}{n^s}$$

is a Dirichlet series. In fact, it is also what we call a Dirichlet L-function.
(iii) Assuming absolute convergence, one can take the product of two Dirichlet series

$$\left(\sum_{m=1}^{\infty} \frac{a_m}{m^s}\right)\left(\sum_{m=1}^{\infty} \frac{b_n}{n^s}\right) = \sum_{n=1}^{\infty}\sum_{n=1}^{\infty} a_m b_n \frac{1}{(mn)^s} = \sum_{N=1}^{\infty} \frac{c_N}{N^s}, c_N = \sum_{d|N} a_d b_{N/d}$$

So for example for $\mathrm{Re}(s) > 2$,

$$\zeta(s-1)\zeta(s) = \left(\sum_{m=1}^{\infty} \frac{m}{m^s}\right)\left(\sum_{m=1}^{\infty} \frac{1}{n^s}\right) = \sum_{N=1}^{\infty} \frac{1}{N^s} \sum_{d|N} d = \sum_{N=1}^{\infty} \frac{\sigma(N)}{N^s}$$

Definition 5.4. The von Mangoldt function $\Lambda : \mathbb{N} \to \mathbb{R}$ is defined by

$$\Lambda(n) = \begin{cases} \log p, \text{ if } n = p^k \text{ for some prime } p \text{ and } k \geq 1 \\ 0, \text{ otherwise} \end{cases}$$

Remark. Λ can be thought of a weighted indicator of the primes. In fact, one can show that the prime numer theorem is equivalent to $\psi(x) \sim x$ where $\psi(x) = \sum_{1 \leq n \leq x} \Lambda(n) \sim x$.

Proposition 5.11. *For* $\mathrm{Re}(s) > 1$,

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

Proof. For $\mathrm{Re}(s) > 1$, we have

$$\log \zeta(s) = \log \prod_{p \text{ prime}} (1 - p^{-s})^{-1} = -\sum_{p \text{ prime}} \log(1 - p^{-s})$$

So

$$\begin{aligned}\frac{\zeta'(s)}{\zeta(s)} = \frac{\mathrm{d}}{\mathrm{d}s}(\log \zeta(s)) &= -\sum_{p \text{ prime}} \frac{p^2 \log p}{1 - p^{-s}} = -\sum_{p \text{ prime}} (\log p) p^{-s} \sum_{k=0}^{\infty} p^{-ks} \\ &= -\sum_{p \text{ prime}} (\log p) \sum_{j=1}^{\infty} p^{-js} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}\end{aligned}$$

as desired. □

Remark. $\psi(x) \sim x$ can be proved by showing

$$\begin{aligned}\psi(x) &= \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \left(-\frac{\zeta'(s)}{\zeta(s)}\right) \frac{x^s}{s} \, \mathrm{d}s \\ &= x - \sum_{0<\mathrm{Re}(\rho)<1, \zeta(\rho)=0} \frac{x^\rho}{\rho} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2} \log\left(1 - \frac{1}{x^2}\right)\end{aligned}$$

for $c > 1$.

5.4 Counting Primes

Proposition 5.12 (Legendre)**.** *Let* $X > 1$ *and* $P = \prod_{p \text{ prime} \le \sqrt{x}} p$*, then*

$$\pi(x) - \pi(\sqrt{x}) + 1 = |\{1 \le n \le x : (n, P) = 1\}| = \sum_{d|P} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor$$

Proof. We make use of the sieve of Eratosthenes. If we delete from $\{2, \ldots, \lfloor x \rfloor\}$ all multiples of primes at most $\sqrt{x}$, we are left with primes in $(\sqrt{x}, x]$, so $\{1 \le n \le x : (n, P) = 1\} = \{1\} \cup \{p : \sqrt{x} < p \le x\}$ which is the first equality.
Also, by Lemma 5.10 we have

$$\begin{aligned}|\{1 \le n \le x : (n, P) = 1\}| &= \sum_{1 \le n \le x} 1_{(n,P)=1} = \sum_{1 \le n \le x} \sum_{d|(n,P)} \mu(d) \\ &= \sum_{d|P} \mu(d) \sum_{1 \le n \le x, d|n} 1 = \sum_{d|P} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor\end{aligned}$$

which is the second equality. □

Theorem 5.13 (Tchebychev)**.** *For any* $x \ge 4$*, we have*

$$\frac{\log 2}{2} \frac{x}{\log x} \le \pi(x) \le 6 \log 2 \frac{x}{\log x}$$

Proof. We shall first show by induction on k that $\pi(2^k) \leq 3 \times 2^k/k$. We will then sandwich x between two consecutive powers of 2.
First note that for even $n \geq 4, \pi(n) \leq n/2$, so $\pi(2^k) \leq 2^{k-1} \leq 3 \times 2^k/k$ for $2 \leq k \leq 6$ (and also for $k = 1$). As for the induction step, observe that when $n \in \mathbb{N}$, we have

$$2^{2n} > N = \binom{2n}{n} = \frac{(2n) \cdot (2n-1) \cdots (n+1)}{n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1} \geq \prod_{p \text{ prime} \in (n,2n]} p \geq n^{\pi(2n)-\pi(n)}$$

So $\pi(2n)-\pi(n) \leq (2\log 2)(n/\log n)$. Therefore, assuming our desired inequality holds for k, then

$$\begin{aligned} \pi(2^{k+1}) &\leq \pi(2^k) + 2\log 2 \frac{2^k}{\log(2^k)} = \pi(2^k) + \frac{2^{k+1}}{k} \\ &\leq \frac{3 \times 2^k}{k} + \frac{2^{k+1}}{k} = \frac{5 \times 2^{k+1}}{2k} \leq \frac{3 \times 2^{k+1}}{k+1} \end{aligned}$$

since $5/(2k) \leq 3/(k+1)$ for $k \geq 5$. This completes the induction. Note that $x/\log x$ is strictly increasing for $x \geq e$. Thus for $4 \leq 2^k < x \leq 2^{k+1}$ for some integer k, we have

$$\pi(x) \leq \pi(2^{k+1}) \leq 6\frac{2^k}{k+1} < 6\frac{2^k}{k} = 6\log 2 \frac{2^k}{\log(2^k)} < 6\log 2 \frac{x}{\log x}$$

which is the desired upper bound.
We need to do some preparation work before we proceed to the proof of the lower bound. □

Definition 5.5. Let $n \geq 1$ and p be a prime. The p-adic valuation $v_p(n)$ of n is the exponent of p in the prime factorisation of n.

Remark. By definition, $n = p^{v_p(n)} n_0$ with $p \nmid n_0$ and $v_p(mn) = v_p(m) + v_p(n)$. In example sheet, you will prove that

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

Lemma 5.14. *Let $n \in \mathbb{N}$ and let $N = \binom{2n}{n}$, then:*
(i) If $2n/3 < p \leq n$, then $(N, p) = 1$.
(ii) If $p^k \mid N$ for some $k \geq 1$, then $p^k \leq 2n$.

Proof. (i) If $p \in (2n/3, n]$, then $p \leq n < 2p \leq 2n < 3p$, so both the numerator and denominator of

$$N = \frac{(2n) \cdot (2n-1) \cdots (n+1)}{n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1}$$

are divisible by exactly one copy of p, hence $(N, p) = 1$.
(ii) Note that

$$v_p(N) = v_p((2n)!) - 2v_p(n!) = \sum_{i=1}^{\infty} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right)$$

But if $x \geq 0$, then $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0, 1\}$, so if $p^k > 2n$, then $\lfloor 2n/p^k \rfloor = 0$, thus

$$v_p(N) = \sum_{i=1}^{k-1} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right) \leq k - 1$$

which means that $p^k \nmid N$. □

Proof of Theorem 5.13 (cont.) By part (ii) of preceding lemma, we know that $p^{v_p(N)} \leq 2n$ for all primes p, hence $v_p(N) \leq \log(2n)/\log p$. Hence

$$\log N = \sum_{p \text{ prime} \leq 2n} v_p(N) \log p \leq \sum_{p \text{ prime} \leq 2n} \frac{\log(2n)}{\log p} \log p = \pi(2n) \log(2n)$$

At the same time, we can obtain a lower bound on N by observing

$$2^{2n} = (1+1)^{2n} = 1 + 1 + \sum_{j=1}^{2n-1} \binom{2n}{j} \leq 2 + (2n-1)N \leq 2nN$$

Combining them,

$$\pi(2n) \log(2n) \geq \log \left(\frac{2^{2n}}{2n} \right) = 2n \log(2) - \log(2n) \implies \pi(2n) \geq \log 2 \frac{2n}{\log(2n)} - 1$$

Hence, if $2n \leq x \leq 2n + 2$, then

$$\pi(x) \geq \pi(2n) \geq \log 2 \frac{2n}{\log(2n)} - 1 \geq \log 2 \frac{x-2}{\log x} - 1 \geq \frac{\log 2}{2} \frac{x}{\log x}$$

which is the desired lower bound. □

5.5 Bertrand's Postulate

Theorem 5.15 (Bertrand's Postulate)**.** *For any $n \in \mathbb{N}$, there is a prime in $[n, 2n)$.*

Lemma 5.16. *For $x \geq 1$, let $P(x) = \prod_{p \text{ prime} \leq x} p$, then $P(x) \leq 4^x$.*

Proof. It suffice to prove this for all natural number $x = n$. We proceed by induction on n. The base cases $n = 2, 3$ are clear. Also note that for $n \geq 1$ we have

$$P(2n+2) = P(2n+1) = P(n+1) \prod_{p \text{ prime} \in [n+2, 2n+1]} p$$

Now, each prime p with $n + 2 \leq p \leq 2n + 1$ divides $\binom{2n+1}{n}$, so we have $\prod_{p \text{ prime} \in [n+2, 2n+1]} p \mid \binom{2n+1}{n}$. Moreover, $2\binom{2n+1}{n} = \binom{2n+1}{n} + \binom{2n+1}{n+1} \leq 2^{2n+1}$. so $\binom{2n+1}{n} \leq 4^n$. It follows that $P(2n+2) = P(2n+1) \leq P(n+1)4^n$ which gives the induction step. □

Proof of Theorem 5.15. Suppose there is no prime $[n, 2n)$. Let $N = \binom{2n}{n}$. Then any prime p that divides N must have $p < n$. By Lemma 5.14(i), if $2n/3 < p \leq$

n, then $(N,p)=1$, so indeed $p \le 2n/3$. Write $N = N_1 N_2$ with $N_1 = \prod_{v_p(N)=1} p$ and $N_2 = \prod_{v_p(N)\ge 2} p^{v_p(N)}$. We have

$$N_1 = \prod_{v_p(N)=1} p \le \prod_{p \text{ prime} \le 2n/3} p = P\left(\frac{2n}{3}\right) \le 4^{2n/3}$$

by the preceding lemma, and

$$N_2 = \prod_{v_p(N)\ge 2} p^{v_p(N)} \le \prod_{p \le \sqrt{2n}} 2n \le (2n)^{\sqrt{2n}}$$

by Lemma 5.14(ii). So

$$\frac{2^{2n}}{2n} \le N = N_1 N_2 \le 4^{2n/3}(2n)^{\sqrt{2n}} \implies \frac{\log 2}{3} 2n \le (1+\sqrt{2n})\log(2n)$$

which is false for $n \ge 2^9$. The case for small n can be check manually (e.g. by the list of primes $p = 2, 5, 11, 23, 47, 89, 179, 359, 719$). □

6 Continued Fractions

6.1 Complete and Partial Quotients

Example 6.1. We want to find a good rational approximation to π in the sense that $|\pi - p/q|$ is small relative to q. We can, of course, approximate π by its expansion in base 10 (or some other bases). We have

$$\left|\pi - \frac{314159}{100000}\right| < 3 \times 10^{-6}$$

But there are something way better, e.g.

$$\left|\pi - \frac{355}{113}\right| < 3 \times 10^{-7}$$

For $\theta \in \mathbb{R}$, we can define a (possibly finite) sequence of integers $a_0, a_1, \ldots$ with $a_n \ge 1$ for all $n \ge 1$ as follows:
Let $a_0 = \lfloor \theta \rfloor$. We stop here if $\theta = a_0$. Otherwise, $0 < \theta - a_0 < 1$, so let $\theta_1 = 1/(\theta - a_0)$, then

$$\theta = a_0 + \frac{1}{\theta_1}$$

Repeat this process with θ_1 gives $a_1 = \lfloor \theta_1 \rfloor$. Again we stop if θ_1 is an integer. Otherwise, take $\theta_2 = 1/(\theta_1 - a_1)$. So we have

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\theta_2}}$$

Repeat again with θ_2, etc., gives our desired sequence. At the n^{th} step, we have an identity of the form

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{\theta_n}}}}} = [a_0, a_1, \ldots, a_{n-1}, \theta_n]$$

If the algorithm terminates there, then $\theta_n = a_n \in \mathbb{Z}_{\geq 1}$ and $\theta = [a_0, a_1, \ldots, a_n]$. If the algorithm does not terminate at all, we write $[a_0, a_1, \ldots]$ to denote the sequence we obtained in this way.

Definition 6.1. We say $[a_0, a_1, \ldots]$ is the continued fraction expansion (CFE) of θ. The integers $a_0, a_1, \ldots$ are known as the partial quotients, the values $\theta_0 = \theta, \theta_1, \ldots$ are known as partial quotients.

Example 6.2. Apply this algorithm on $\theta = 59/13$ gives

$$\frac{59}{13} = 4 + \frac{7}{13} = 4 + \cfrac{1}{1 + \cfrac{6}{7}} = 4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6}}}$$

So $59/13 = [4, 1, 1, 6]$.

Proposition 6.1. *The CFE of θ terminates iff $\theta \in \mathbb{Q}$.*

Proof. The "only if" part is trivial. Conversely, observing that the numerators in the minimal fraction of θ_i is strictly decreasing with i, hence must hit 1 eventually. □

Remark. 1. If the CFE of $\theta \in \mathbb{Q}$ terminates at the n^{th} step, then $a_n = \theta_n \geq 2$.
2. The continued fraction algorithm for $a \in \mathbb{Q}$ is essentially the Euclid's algorithm on p, q where $a = p/q, (p, q) = 1$

Example 6.3. Let $\theta = 59/13$, then Euclid's algorithm gives

$$59 = 4 \times 13 + 7 \tag{1}$$
$$13 = 1 \times 7 + 6 \tag{2}$$
$$7 = 1 \times 6 + 1 \tag{3}$$
$$6 = 6 \times 1 + 0 \tag{4}$$

and $[4, 1, 1, 6]$ is exactly the continued fraction expansion of θ.
Note also that the expansion produces successive approximation to θ by

$$[a_0] = a_0 = 4$$
$$[a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = 5$$
$$[a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + a_2^{-1}} = \frac{a_2(a_0 a_1 + 1) + a_0}{a_1 a_2 + 1} = 9/2$$
$$[a_0, a_1, a_2, a_3] = 59/13$$

This motivates our new definition of convergents.

6.2 Convergence of Convergents

Definition 6.2. Let $a_0, a_1, a_2, \ldots$ be integers with $a_n \geq 1$, then for any $n \geq 1$, we define the convergents $(p_n/q_n)_{n\geq 0}$ of the CFE $[a_0, a_1, \ldots]$ as pairs of integers $(p_n, q_n)_{n\geq 0}$ given by the recursion

$$\begin{cases} p_0 = a_0 \\ q_0 = 1 \end{cases}, \begin{cases} p_1 = a_0 a_1 + 1 \\ q_1 = a_1 \end{cases}, \begin{cases} p_n = a_n p_{n-1} + p_{n-2} \\ q_n = a_n q_{n-1} + q_{n-2} \end{cases}, n \geq 2$$

Remark. (i) $1 \leq q_1 < q_2 < q_3 < \cdots$.
(ii) It is convenient to define $p_{-1} = 1, q_{-1} = 0$ so that one can start the recursion from $n = 1$.
(iii) We can also write the recursion in matrix form

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}$$

(iv) We employed a small confusion of notation here: When we write the convergent p_n/q_n, what we really mean (and indeed, what we've really defined) is the pair of integers (p_n, q_n) instead of their fraction. The reason we do it will become abundantly clear after the next proposition.
Since we will make use of both the integers p_n, q_n themselves and their fractions in our later discussions, we will implicitly mean both when we write p_n/q_n (but it should be clear from the context when we actually use it as a fraction).

Proposition 6.2. *Let $(p_n/q_n)_{n\geq -1}$ be convergents of the CFE $[a_0, a_1, \ldots]$, then:*
(i) $(p_n, q_n) = 1$. In fact, $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1}$.
(ii) $[a_0, \ldots, a_n] = p_n/q_n$.
(iii) If $\alpha = [a_0, \ldots, a_n, \beta]$ for some $n \geq 0$ and real $\beta > 0$, then $\alpha = (p_n\beta + p_{n-1})/(q_n\beta + q_{n-1})$ and α lies strictly between p_n/q_n and p_{n-1}/q_{n-1}.

Proof. (i) Take determinants in both side of the identity in the last part of the remark.
(ii) Follows from (iii).
(iii) Induction on n. The base case is trivial. For $n > 0$, let $\gamma = a_n + \beta^{-1}$, then

$$\begin{aligned} \alpha = [a_0, a_1, \ldots, a_{n-1}, \gamma] &= \frac{p_{n-1}\gamma + p_{n-2}}{q_{n-1}\gamma + q_{n-2}} = \frac{p_{n-1}(\beta a_n + 1) + \beta p_{n-2}}{q_{n-1}(\beta a_n + 1) + \beta q_{n-2}} \\ &= \frac{(a_n p_{n-1} + p_{n-2})\beta + p_{n-1}}{(a_n q_{n-1} + q_{n-2})\beta + q_{n-1}} = \frac{p_n\beta + p_{n-1}}{q_n\beta + q_{n-1}} \end{aligned}$$

The size estimate follows from the fact that for $y, y' > 0$ and $x/y < x'/y'$, we have $x/y < (x + x')/(y + y') < x'/y'$. □

Theorem 6.3. *Let $\theta \in \mathbb{R}$ be irrational with CFE $[a_0, a_1, \ldots]$, then for any $n \geq 0$, we have*

$$\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}$$

In particular, $p_n/q_n \to \theta$ as $n \to \infty$.

Proof. From the preceding proposition, we know that

$$\left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \left|\frac{p_n q_{n+1} - p_{n+1} q_n}{q_n q_{n+1}}\right| = \frac{1}{q_n q_{n+1}}$$

and that

$$\theta = [a_0, \ldots, a_{n+1}, \theta_{n+2}] \in \left(\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}\right)$$

Combining them gives the size estimate. We also know that $q_n \to \infty$ as $n \to \infty$, so $|\theta - p_n/q_n| \to 0$ or $p_n/q_n \to \theta$ as $n \to \infty$. □

Remark. (i) As a result, it makes sense to write $\theta = \lim_{n\to\infty}[a_0, \ldots, a_n]$.
(ii) One can show that $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$ and that the sequences $(p_{2n}/q_{2n})_{n\geq 1}, (p_{2n-1}/q_{2n-1})_{n\geq 1}$ are strictly increasing and strictly decreasing respectively.
(iii) If we fix a denominator $q \geq 1$ and try to minimise $|\theta - p/q|$, then the best we can expect in general is $|\theta - p/q| \leq 1/(2q)$ with p being the closest integer to $q\theta$. Hence the convergents approximate θ very well indeed.

Theorem 6.4. *Let θ be irrational and suppose that $(p_n/q_n)_{n\geq -1}$ are the convergents for the CFE of θ, then:*
(i) Suppose $q \in \mathbb{N}$ is such that $1 \leq q < q_{n+1}$ for some n, then for any $p \in \mathbb{Z}$ we have $|q\theta - p| \geq |q_n\theta - p_n|$.
(ii) Moreover, if $q \in \mathbb{N}$ and $p \in \mathbb{Z}$ are such that $|\theta - p/q| < |\theta - p_n/q_n|$, then $q > q_n$.

Proof. (i) clearly implies (ii) since for any $q \leq q_n < q_{n+1}$ we would have

$$\left|\theta - \frac{p}{q}\right| = \frac{1}{q}|q\theta - p| \geq \frac{1}{q}|q_n\theta - p_n| = \frac{q_n}{q}\left|\theta - \frac{p_n}{q_n}\right| \geq \left|\theta - \frac{p_n}{q_n}\right|$$

assuming (i).
To prove (i), let $q \in \mathbb{N}, p \in \mathbb{Z}$ with $1 \leq q < q_{n+1}$ for some $n \in \mathbb{N}$. Consider the system of equations

$$\begin{cases} p_n u + p_{n+1} v = p \\ q_n u + q_{n+1} v = q \end{cases}$$

We know that $p_n q_{n+1} - p_{n+1} q_n = (-1)^n$, so the system has a unique solution $(u, v) \in \mathbb{Z}^2 - \{(0,0)\}$. Thus

$$q\theta - p = (q_n u + q_{n+1} v)\theta - (p_n u + p_{n+1} v) = (q_n\theta - p_n)u + (q_{n+1}\theta - p_{n+1})v$$

If $v = 0$, then $q\theta - p = (q_n\theta - p_n)u$ which implies the result since $|u| \geq 1$. Assume henceforth that $v \neq 0$. Since $q_n u = q - q_{n+1} v$, u, v must have opposite signs since $0 < q < q_{n+1}$. In particular, $u \neq 0$. Recall that $\theta - p_n/q_n, \theta - p_{n+1}/q_{n+1}$ also have opposite signs. It follows that $(q_n\theta - p_n)u$ and $(q_{n+1}\theta - p_{n+1})v$ have the same sign. Hence $|q\theta - p| = |(q_n\theta - p_n)u| + |(q_{n+1}\theta - p_{n+1})v| \geq |q_n\theta - p_n|$ since u is nonzero. □

Theorem 6.5. *Let θ be irrational and suppose that $(p_n/q_n)_{n\geq -1}$ are convergents of the CFE of θ, then:*
(i) At least one of any pair of consecutive convergents satisfies

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

(ii) If $p/q \in \mathbb{Q}$ has $|\theta - p/q| < 1/(2q^2)$, then $p/q = p_n/q_n$ for some $n \in \mathbb{N}$.

Proof. (i) Suppose there is some $n \in \mathbb{N}$ such that

$$\left|\theta - \frac{p_n}{q_n}\right| \geq \frac{1}{2q_n^2}, \left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| \geq \frac{1}{2q_{n+1}^2}$$

Then

$$\frac{1}{2}\left(\frac{1}{q_n^2} + \frac{1}{q_{n+1}^2}\right) \leq \left|\theta - \frac{p_n}{q_n}\right| + \left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \frac{1}{q_n q_{n+1}}$$

which contradicts the AM-GM inequality.
Suppose $p/q \in \mathbb{Q}$ is such that $|\theta - p/q| < 1/(2q^2)$. Choose $n \geq 0$ such that $q_n \leq q < q_{n+1}$. If $p/q \neq p_n/q_n$, then

$$\frac{1}{qq_n} \leq \left|\frac{p}{q} - \frac{p_n}{q_n}\right| \leq \left|\theta - \frac{p}{q}\right| + \left|\theta - \frac{p_n}{q_n}\right| = \frac{1}{q}|q\theta - p| + \frac{1}{q_n}|q_n\theta - p_n|$$

But $|q\theta - p| \geq |q_n\theta - p_n|$ by the preceding theorem, so

$$\frac{1}{qq_n} \leq \left(\frac{1}{q} + \frac{1}{q_n}\right)|q\theta - p| < \frac{1}{2q^2} + \frac{1}{2qq_n} \implies q < q_n$$

Contradiction. □

Example 6.4. We want to expand $\theta = \sqrt{6}$ as continued fraction. Indeed,

$$\theta = \sqrt{6} + 2 + (\sqrt{6} - 2) \implies a_0 = 2$$

$$\theta_1 = \frac{1}{\sqrt{6} - 2} = \frac{\sqrt{6} + 2}{2} = 2 + \frac{\sqrt{6} - 2}{2} \implies a_1 = 2$$

$$\theta_2 = \frac{2}{\sqrt{6} - 2} = \sqrt{6} + 2 = 4 + \sqrt{6} - 2 \implies a_2 = 4$$

$$\theta_3 = \frac{1}{\sqrt{6} - 2} = \theta_1$$

So $a_1 = a_3 = \cdots = 2$ and $a_2 = a_4 = \cdots = 4$, i.e. θ has continued fraction $[2, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, \ldots]$.

6.3 Periodic Continued Fractions

Definition 6.3. A CFE is called eventually periodic if it has the form

$$[a_0, a_1, \ldots, a_m, \ldots, a_{m+k-1}, a_m, \ldots, a_{m+k-1}, a_m, \ldots]$$

for some $m, k \in \mathbb{Z}_{\geq 0}$. It is called purely periodic if it can be written in the said form with $m = 0$. The period of an eventually periodic CFE is the least positive integer k such that it can be written in the said form.

For an eventually periodic CFE, we often use the abbreviated notation $[a_0, a_1, \ldots, a_{m-1}, \overline{a_m, \ldots, a_{m+k-1}}]$. Like in the last example, if the sequence of complete quotients of an irrational number eventually repeats, then its CFE is eventually periodic.

Example 6.5. $\sqrt{6} = [2, \overline{2, 4}]$.

Theorem 6.6 (Lagrange)**.** *The CFE of an irrational θ is eventually periodic if and only if θ is a quadratic irrational, i.e. the root of a quadratic polynomial with rational coefficents.*

Proof. Suppose $\phi = [\overline{a_0, a_1, \ldots, a_n}]$, then $\phi = [a_0, a_1, \ldots, a_n, \phi] = (p_n\phi + p_{n-1})/(q_n\phi + q_{n-1})$ by Proposition 6.2, which means that $q_n\phi^2 + (q_{n-1} - p_n)\phi - p_{n-1} = 0$, i.e. ϕ is a quadratic irrational.
Suppose $\theta = [a_0, \ldots, a_{m-1}, \overline{a_m, \ldots, a_{m+k-1}}] = [a_0, \ldots, a_{m-1}, \phi]$ is eventually periodic where $\phi = [\overline{a_m, \ldots, a_{m+k-1}}]$ is known to be a quadratic irrational. Then $\theta = (p_{m-1}\phi + p_{m-2})/(q_{m-1}\phi + q_{m-2})$ need also be a quadratic irrational.
Conversely, suppose θ is a quadratic irrational, i.e. it is a solution to $A\theta^2 + B\theta + C = 0$ for some $A, B, C \in \mathbb{Z}$. Consider the BQF $f = (A, B, C)$. Let θ' be the conjugate root to θ (i.e. the other root to the quadratic), then $B = -A(\theta + \theta'), C = A\theta\theta'$. Note that $f(\theta, 1) = 0$. Now for each $n \geq 0$, we define a BQF $f_n(x, y) = f(p_n x + p_{n-1}y, q_n x + q_{n-1}y) = (A_n, B_n, C_n)$ which share the same discriminant as f since $p_n q_{n-1} - p_{n-1}q_n = \pm 1$. By Proposition 6.2, we have $\theta = (p_n\theta_{n+1} + p_{n-1})/(q_n\theta_{n+1} + q_{n-1})$, so $f_n(\theta_{n+1}, 1) = f(p_n\theta_{n+1} + p_{n-1}, q_n\theta_{n+1} + q_{n-1}) = (q_n\theta_{n+1} + q_{n-1})^2 f(\theta, 1) = 0$.
Finally, observe that there is some $K > 0$ such that $|f(p_n, q_n)| \leq K$ for all n. Indeed, by Theorem 6.3

$$|f(p_n, q_n)| = q_n^2 \left| f\left(\frac{p_n}{q_n}, 1\right)\right| = Aq_n^2 \left|\frac{p_n}{q_n} - \theta\right| \left|\frac{p_n}{q_n} - \theta'\right| \leq A\left|\frac{p_n}{q_n} - \theta'\right| \to A|\theta - \theta'|$$

as $n \to \infty$. It follows that $f_n(1, 0) = f(p_n, q_n) = A_n$ and $f_{n+1}(0, 1) = f(p_n, q_n) = C_{n+1}$ are both bounded by K, i.e. A_n, C_n only have finitely many choices. But the discriminant of f_n is fixed, so in fact A_n, B_n, C_n all have only finitely many choices, so $\{f_n\}$ is finite. Since θ_n is one of at most two roots of $f_{n-1}(x, 1)$, the set of complete quotients $\{\theta_n\}$ is finite, i.e. $\theta_0, \theta_1, \theta_2, \ldots$ eventually repeats, hence θ is eventually periodic. □

One can actually prove that

Theorem 6.7 (Galois)**.** *Let θ be a quadratic irrational. Then the CFE of θ is purely periodic if and only if $\theta > 1$ and $-1 < \theta' < 0$ where θ' is the conjugate root to θ.*

Corollary 6.8. *If $d \in \mathbb{N}$ is not a square, then $\sqrt{d} = [a_0, \overline{a_1, \ldots, a_n}]$.*

Proof. $\theta_1 = 1/(\sqrt{d} - a_0) > 1$ with its conjugate root $1/(-\sqrt{d} - a_0) \in (-1, 0)$, so θ_1 is purely periodic. □

Remark. In fact, $\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}]$.

Theorem 6.9 (Pell's Equation)**.** *If $d \in \mathbb{N}$ is not a square, then $x^2 - dy^2 = 1$ has a solution $(x, y) \in \mathbb{Z}^2$ with $xy \neq 0$.*

Proof. Let $\theta = \sqrt{d} = [a_0, \overline{a_1, \ldots, a_n}] = [a_0, a_1, \ldots, a_n, \theta_{n+1}]$ with $\theta_1 = \theta_{n+1} = [\overline{a_1, \ldots, a_n}]$. Assume n is even (if not we can replace n by $2n$). Note that $\theta = a_0 + 1/\theta_1$, so $1/\theta_1 = \theta - a_0$, i.e.

$$\sqrt{d} = \frac{p_n\theta_1 + p_{n-1}}{q_n\theta_1 + q_{n-1}} = \frac{p_n + p_{n-1}(-\sqrt{d} - a_0)}{q_n + q_{n-1}(\sqrt{d} - a_0)}$$

Thus $q_{n-1}d+(q_n-q_{n-1}a_0)\sqrt{d} = p_n - a_0p_{n-1}+p_{n-1}\sqrt{d}$. Comparing coefficients, we find $p_{n-1} = q_n - q_{n-1}a_0, q_{n-1}d = p_n - a_0p_{n-1}$, consequently $p_{n-1}^2 - dq_{n-1}^2 = p_{n-1}q_n - q_{n-1}p_n = (-1)^n = 1$ and we are done. □

This in fact shows that $x^2 - dy^2 = 1$ has infinitely many solutions. It also shows that if $\sqrt{d}$ has odd period, then we can solve $x^2 - dy^2 = -1$ (infinitely many times) as well.

Example 6.6. (i) We want to solve $x^2 - 6y^2 = 1$ in the nonzero integers. Write $\sqrt{6} = [2, \overline{2, 4}]$, then $p_1/q_1 = [a_0, a_1] = [2, 2] = 2 + 1/2 = 5/2$, so $(x, y) = (5, 2)$ is a solution. We can repeat the period to find more solutions: $p_3/q_3 = 49/20$, so $(49, 20)$ is another solution.
(ii) $x^2 - 17y^2 = -1$. We have $\sqrt{17} = [4, \overline{8}]$. $p_0/q_0 = 4/1 = 4$, so $(4, 1)$ is a solution.

Remark. Indeed, one can prove that any solution to Pell's equation must be a convergent of $\sqrt{d}$ using Theorem 6.5.

7 Primality Testing and Prime Factorisation

Given a (large) integer N, we want to know methods to detemrine efficiently if N is prime. If N is not prime, then we want an algorithm to find a non-trivial prime-factor efficiently. We usually assume N is odd since axing away powers of 2 is easy.
It turns out that primality testing can be done in polynomial time, but there has not been any polynomial-time factorisation algorithm so far. However, we will see some algorithms that are a lot better than the obvious algorithms.

7.1 The Solovay-Strassen Test

We shall first produce an algorithm by exploiting Fermat's little theorem. Recall that if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$. A natural idea is to fix a and look at $a^{N-1} \bmod N$. It can surely sieve out some non-primes while retaining all primes, but does it suffice in general? Alas, no.

Example 7.1. 1. Take $N = 15$. Consider $a = 2$, then $2^{14} \equiv 4 \pmod{15}$, so 15 is not prime by this test.
2. Take $N = 91$. N is composite, but $3^{90} \equiv 1 \pmod{91}$ – so the test fails to exclude it when we take $a = 3$. However, if we choose $a = 2$, then $2^{90} \equiv 64 \pmod{91}$ does give the desired contradiction.

Definition 7.1. Let $b \in \mathbb{N}$. An odd composite number $N > 1$ is said to be a Fermat pseudorprime to base b if $(b, N) = 1$ and $b^{N-1} \equiv 1 \pmod{N}$.

This definition obviously only depends on N and $b \bmod N$, so it suffices to consider bases $1 \leq b \leq N$.

Example 7.2. 91 is a Fermat pseudoprime to base 3 but not to base 2.

Proposition 7.1. *Let $N > 1$. If N is not a Fermat pseudoprime to some base b_0, then it is not a Fermat pseudoprime to base b for at least half of $b \in (\mathbb{Z}/NZ)^\times$.*

Proof. The set

$$B = \{1 \leq b < N : (b, N) = 1, N \text{ is a Fermat pseudoprime to base } b\}$$

is clearly a subgroup of $(\mathbb{Z}/NZ)^\times$. It's proper as $b_0 \in (\mathbb{Z}/NZ)^\times$ is not in B. Consequently $|B| \leq |(\mathbb{Z}/NZ)^\times|/2$ which concludes the proof. □

Remark. The proposition means that if N is not a Fermat pseudoprime to some bases, then we can determine one of these bases by doing a relatively small amount of guesses. Sadly, there are composite numbers that are pseudoprimes to every base.

Definition 7.2. An odd composite integer $N > 1$ is said to be a Carmichael number if it is a Fermat pseudoprime to every base.

Remark. Unfortunately, there has been shown to be infinitely many Carmichael numbers.

A tiny bit more sophisticated way to extend this idea is by recalling that if p is prime and $(a, p) = 1$, then $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Definition 7.3. Let $b \in \mathbb{N}$. An odd composite integer $N > 1$ is said to be an Euler pseudoprime to base b if $b^{(N-1)/2} \equiv \left(\frac{b}{N}\right) \pmod{N}$.

Remark. Every Euler pseudoprime is in particular a Fermat pseudoprime (to the same base).

Proposition 7.2. *Let $N > 1$. If N is not an Euler pseudoprime to some base b_0, then it is not an Euler pseudoprime to at least half the bases in $(\mathbb{Z}/N\mathbb{Z})^\times$.*

Proof. Identical to the proof of Proposition 7.1. □

Theorem 7.3. *Let $N > 1$. If N is odd and composite, there there is a base $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that N is not an Euler pseudoprime to base b.*

Proof. Let $N > 1$. Suppose first that N is square-free. Let $N = pm$ with p a prime and $m \geq 3, p \nmid m$. Pick $u \in \mathbb{Z}$ such that $\left(\frac{u}{p}\right) = -1$, then by the Chinese remainder theorem there is some $b \geq 1$ such that $b \equiv u \pmod{p}, b \equiv 1 \pmod{m}$ which has $\left(\frac{b}{N}\right) = -1$. But $b^{(N-1)/2} \equiv 1 \not\equiv -1 \pmod{m}$, so $b^{(N-1)/2} \not\equiv -1 \equiv \left(\frac{b}{N}\right) \pmod{N}$, so N is not an Euler pseudoprime to base b.
If N is not square-free, then choose prime p such that $p^2 \mid N$. We have $(1 + p)^{N-1} \equiv 1 + (N-1)p \not\equiv 1 \pmod{p^2}$. By the Chinese remainder theorem, there is some $b \in \mathbb{Z}$ with $(b, N) = 1$ such that $b \equiv 1 + p \pmod{p^2}$. Then $b^{N-1} \not\equiv 1 \pmod{p^2}$, so $b^{(N-1)/2} \not\equiv \pm 1 \pmod{N}$, i.e. N is not an Euler pseudoprime to base b. □

This gives rise to a primality testing algorithm by testing whether $a^{(p-1)/2} \equiv \left(\frac{a}{N}\right) \pmod{N}$ for each a. In practice, however, we are sometimes willing to trade some degree of sufficiency to efficiency.
The Solovay-Strassen primality test goes as follows: Given an odd $N > 1$, pick $1 < b < N$ at random. First check if $(b, N) = 1$ with Euclid's algorithm. If this fails, then N is already composite. Otherwise, compute $b^{(N-1)/2}$ by repeated squaring and $\left(\frac{b}{N}\right)$ by the reciprocity law and $b^{(p-1)/2} \equiv \left(\frac{b}{N}\right) \pmod{N}$. If this fails, N is composite. If this does not fail, then we repeat the process unless we are satisfied with the number of iterations that have been done. If N passes k iterations of this test, then N is composite with probability at most $1/2^k$.

7.2 The Miller-Rabin Test

Can we push this idea further? If p is an odd prime and $p \nmid a$, then $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. If indeed $a^{(p-1)/2} \equiv 1 \pmod{p}$ and $(p-1)/2$ is even, then $a^{(p-1)/4} \equiv \pm 1 \pmod{p}$, and so on. So if p is a prime, then either there is some $r \geq 1$ such that $a^{(p-1)/2^r} \equiv -1 \pmod{p}$ for some r, or $a^{(p-1)/2^r} \equiv 1 \pmod{p}$ and $(p-1)/2^r$ is odd. This motivates the following:

Definition 7.4. Let $N > 1$ be odd and let $b \in \mathbb{N}$ with $(b, N) = 1$. Write $N - 1 = 2^s t$ for t odd, $s \geq 1$. We say that N passes the strong test to base b if either $b^t \equiv 1 \pmod{N}$ or $b^{2^r t} \equiv -1 \pmod{N}$ for some $0 \leq r < s$.
If N passes the strong test to base b, then we say that N is a strong pseudoprime to base b.

Remark. If N is prime, then it will always pass the strong test to base b for any base b with $(b, N) = 1$.

Example 7.3. Let $N = 65$ and $b = 8$. Then $N - 1 = 2^6$, so $s = 6$ and $t = 1$. Now $8^2 \equiv -1 \pmod{65}$, so 65 is a strong pseudoprime to base 8.
But if we take instead $b = 2$, then $2^1 \not\equiv \pm 1 \pmod{65}$ and $2^{2^r} \not\equiv -1 \pmod{65}$ for any $r \in \{1, \ldots, 5\}$, so 65 fails the strong test to base 2 and is therefore composite.

Remark. It can be shown that:
1. If N is a strong pseudoprime, then it is an Euler and hence Fermat psueoprime (to the same base). In particular, any odd composite N must fail at least one of the strong tests.
2. If N is odd and composite, then it passes the strong test for at most a quarter of bases $b \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Consequently, we are able to formulate the Miller-Rabin primality test: Given odd $N > 1$, pick $1 < b < N$ at random. Check first whether $(b, N) = 1$. If not then N is composite, otherwise perform the strong test to base b. If this fails, then N is composite. If N passes the above test k times, then N is composite with probability at most $1/4^k$.

Remark. 1. Assuming the generalised Riemann Hypothesis (which postulates that the Dirichlet L-series have no zeros in the region $\mathrm{Re}(s) > 1/2$), if N is composite, then it fails the strong test to base b for some $b < 2(\log N)^2$. Since the strong test can be performed in polynomial time, this gives a polynomial-time deterministic primality test.
2. There is a deterministic polynomial-time primality test found by Agrawal-Kayal-Saxena (2002).

7.3 The Factor Base Method

We now turn to factorisation algorithms. Suppose $N = ab$ with $|a - b|$ nonzero and preferably small, then we have the identity

$$N = ab = r^2 - s^2, r = \frac{a+b}{2} > \sqrt{N}, s = \frac{|a-b|}{2}$$

The idea is to try $r = \lfloor \sqrt{N} \rfloor + 1, \lfloor \sqrt{N} \rfloor + 2, \ldots$ and see if $r^2 - N$ is a square. If so, say $r^2 - N = s^2$, then $N = (r+s)(r-s)$ factors N. This is known as Fermat factorisation algorithm.

Example 7.4. Let $N = 200819$. Note that $\lfloor\sqrt{200819}\rfloor = 448$, so we start at 449. $449^2 - N = 782$ is not a square, so we continue with 450. $250^2 - N = 1681 = 41^2$ is a square, so $N = (450 + 41)(450 - 41) = 491 \times 409$.

Remark. We could have looped over s instead, but it would usually take longer. In general, if $N = ab$ with $a > b$, then the number of steps is bounded by $(a - b)/2$.

Many modern ways of factorisation are based on a generalisation of Fermat factorisation, namely:

Proposition 7.4. *Suppose $x^2 \equiv y^2 \pmod N$ and $x \not\equiv \pm y \pmod N$, then $(N, x - y)$ and $(N, x + y)$ are nontrivial factors of N.*

Proof. $N \nmid (x \pm y)$, so $(N, x \pm y) \neq N$; $N \mid (x + y)(x - y)$, so $(N, x \pm y) \neq 1$. □

Remark. Finding congruent squares directly is not much easier than Fermat factorisation. Instead, we will use the idea of finding several x_i such that $x_i^2 \equiv c_i \pmod N$ where c_i only has small prime factors, and multiply some of these congruences to get the desired congruent squares using the next lemma.

Lemma 7.5. *Let $p_1, \ldots, p_r$ be distinct primes and $c_1, \ldots, c_k$ be nonzero integers whose only prime factors are in $\{p_i : i = 1, \ldots, r\}$. Then for any $k > r + 1$, there is a nonempty set $I \subset \{1, \ldots, k\}$ such that $\prod_{i \in I} c_i$ is a square.*

Proof. For $J \subset \{1, \ldots, k\}$ we write

$$c_J = \prod_{i \in J} c_i = (-1)^{\alpha_{J,0}} p_1^{\alpha_{J,1}} \cdots p_r^{\alpha_{J,r}} m_J^2$$

where $m_J \geq 1$ and $\alpha_{J,0}, \ldots, \alpha_{J,r} \in \{0, 1\}$. Consider the collection of $(r + 1)$-tuples $\underline{\alpha}_J = (\alpha_{J,0}, \ldots, \alpha_{J,r}) \in \{0, 1\}^{r+1}$ which has at most 2^{r+1} choices. There are $2^k > 2^{r+1}$ possible subsets $J \subset \{1, \ldots, k\}$, so there are subsets $J \neq K$ such that $\underline{\alpha}_J = \underline{\alpha}_K$. This makes $c_J c_K$ a square. Consequently, c_I would also be a square where $I = (J - (J \cap K)) \cup (K - (J \cap K))$ ($I \neq \varnothing$ as $J \neq K$). □

Definition 7.5. A factor base is a set $B = \{-1, p_1, \ldots, p_r\}$ where the p_i are distinct primes. A B-number is a positive integer x such that the unique integer $\langle x^2 \rangle$ in $(-N/2, N/2)$ congruent to x^2 mod N is divisible only by primes in B.

The factor base method of factorisation is as follows: First, choose a factor base B and generate enough B-numbers $\{x_i\}$. Find a subset I of indices such that $\prod_{i \in I} \langle x_i^2 \rangle = y^2$ is a square. Then $x^2 \equiv y^2 \pmod N$ where $x = \prod_{i \in I} x_i$. If $x \not\equiv \pm y \pmod N$ we have found a factor of N. Otherwise, we find some more B-numbers and try again.

Remark. 1. We shall see two methods for finding B-numbers: The first is to try $x_i = \lfloor\sqrt{kN}\rfloor$ or $\lfloor\sqrt{kN}\rfloor + 1$ for small $k \geq 1$ as x_i^2 is expected to be not too far from a multiple of N. Another method is to use continued fractions, which we shall discuss later.
2. In practice, we usually generate some x_i's first as candidates before choosing the factor base B.
3. Lemma 7.5 guaranteed the existence of the subset I, but the naive approach to compute it is not a polynomial-time algorithm. Tools in linear algebra will

allow us to find a polynomial-time algorithm for it.
4. Why is this algorithm sufficient? Heuristically, suppose $N = \prod_{i=1}^{t} p_i^{e_i}$ where $e_i \geq 1$ and p_i are distinct primes, then $x^2 \equiv 1 \pmod{p_i^{e_i}}$ has solutions ± 1, so by Chinese remainder theorem $x^2 \equiv 1 \pmod{N}$ has 2^t distinct solutions. Two of these are ± 1, so the procedure is successful if x, y are such that $xy^{-1} \pmod{N}$ is one of the $2^t - 2$ nontrivial solutions. This happens with probability $1 - 1/2^{t-1}$, so this should eventually work if $t \geq 2$. When $t = 1$, N is easy to factor: Just compute the integer x closest to $\sqrt[n]{N}$ for $2 \leq n \leq (\log N)/(\log 3)$ and check if $x^n = N$.

Example 7.5. Let $N = 1829$. We pick the factor base

$$B = \{-1, 2, 3, 5, 7, 11, 13, 19\}$$

Note that $\lfloor \sqrt{1829k} \rfloor = 42, 60, 74, 85$ for $k = 1, 2, 3, 4$. Using these, we have

x_i	42	43	60	61	74	75	85
$\langle x_i^2 \rangle$	-65	20	-58	63	-11	138	-91
Factorisation	$-5 \cdot 13$	$2^2 \cdot 5$	$-2 \cdot 29$	$3^2 \cdot 7$	-11	$2 \cdot 3 \cdot 23$	$-7 \cdot 13$
B-number?	Yes	Yes	No	Yes	Yes	No	Yes

So we want $\{x_i\}_i = \{42, 43, 61, 74, 85\}$. By inspection, $(42 \cdot 43 \cdot 61 \cdot 85)^2 \equiv (-5 \cdot 13)(2^2 \cdot 5)(3^2 \cdot 7)(-7 \cdot 13) \equiv (2 \cdot 3 \cdot 5 \cdot 7 \cdot 13)^2 \pmod{N}$, so $(1459)^2 \equiv 901^2 \pmod{1829}$, therefore we have found nontrivial factors $(1829, 1459 - 901) = 31, (1829, 1459 + 901) = 59$.

Remark. In this case, we do have $N = (N, x + y)(N, x - y)$ which doesn't need to be the case in general.

What about the method using continued fractions?

Lemma 7.6. *Let p_n/q_n be a convergent of $\sqrt{N}$, then $|p_n^2 - Nq_n^2| \leq 2\sqrt{N}$.*

Proof.

$$\begin{aligned} |p_n^2 - Nq_n^2| = q_n^2 \left| \sqrt{N} - \frac{p_n}{q_n} \right| \left| \sqrt{N} + \frac{p_n}{q_n} \right| &\leq \frac{q_n}{q_{n+1}} \left(2\sqrt{N} + \frac{1}{q_n q_{n+1}} \right) \\ = \frac{1}{q_{n+1}} \left(2q_n \sqrt{N} + \frac{1}{q_{n+1}} \right) &< \frac{1}{q_{n+1}} (2q_n + 1)\sqrt{N} \leq 2\sqrt{N} \end{aligned}$$

by Theorem 6.3. □

Remark. 1. In particular, $\langle p_n^2 \rangle = \langle p_n^2 - Nq_n^2 \rangle = p_n^2 - Nq_n^2$, so p_n is a good B-number candidate.
2. In the computation of $p_n = a_n p_{n-1} + p_{n-2}$, we can work modulo N at each step since we only need $p_n \bmod N$.

Example 7.6. Let $N = 12403$. We have $\sqrt{N} = [111, 2, 1, 2, 2, 7, 1, \ldots]$.

$p_n \bmod N$	111	223	334	891	2116	3300	5416
$\langle p_n^2 \rangle$	-82	117	-71	89	-27	166	-39
Factorisation	$-2 \cdot 41$	$3^2 \cdot 13$	-71	89	-3^3	$2 \cdot 83$	$-3 \cdot 13$

which calls for $B = \{-1, 3, 13\}$. If we take this factor base, then the B-numbers in this list are $223, 2116$ and 5416.
By inspection, $(223 \cdot 2116 \cdot 5416)^2 \equiv (3^2 \cdot 13)(-3^3)(-3 \cdot 13) \equiv (3^3 \cdot 13)^2 \pmod{N}$, so $11341^2 \equiv 351^2 \pmod{12403}$ which gives factors $(12403, 11341 - 351) = 157, (12403, 11341 + 351) = 79$.

Remark. 1. A generalisation of this is known as the "number field sieve" which is the the best known factorisation algorithm we have so far. It runs in subexponential time $O(\exp(c(\log N)^{1/3}(\log\log N)^{2/3}))$ for a constant $c > 0$.
2. If we are seeking factors of a particular "shape", we can make things quicker. One example of this will be introduced in the next section.

7.4 Pollard's $p - 1$ Method

Suppose $N = pN_0$ with $(p, N_0) = 1$ and that $p - 1$ is a product of small primes. Consider $a^{p-1} \pmod{N}$ for some a. We have $a^{p-1} \equiv 1 \pmod{p}$, but likely $a^{p-1} \not\equiv 1 \pmod{N_0}$, so $(a^{p-1} - 1, N)$ is likely a nontrivial factor of N. However, we do not know p in advance. But notice that $a^k \equiv 1 \pmod{p}$ whenever k is a multiple of $p - 1$, so if $p - 1$ is a product of small primes, we can construct a suitable k to replace the $p - 1$ in above.
Pollard's $p - 1$ method does the following: Suppose $N = pN_0$ with $(p, N_0) = 1$ and that $p - 1$ is a product of small primes. Let $k = \operatorname{lcm}(1, 2, \ldots, m)$, then k is divisible by all prime powers at most m. Choose a random, small $a \geq 2$. If $(a, N) > 1$ then we are done. Otherwise, compute $a^k \bmod N$ by repeated squaring and find $(a^k - 1, N)$ and hope it is a nontrivial factor of N. This would work if all prime powers dividing $p - 1$ are at most m, in which case we would have $p - 1 \mid k$ and thus $a^k \equiv 1 \pmod{p}$.

Example 7.7. Let $N = 540143$. Try $k = \operatorname{lcm}(1, 2, \ldots, 8) = 840$ and $a = 2$, then $2^k = 2^{105 \times 8} = (2^{64+32+8+1})^8 \equiv 53047 \pmod{N}$ and $(53047 - 1, 540143) = 421 = p$ is a nontrivial of N (note that $p - 1 = 2^2 \cdot 3 \cdot 5 \cdot 7$ is indeed a product of small primes). Indeed $N = 421 \cdot 1283$.

Remark. 1. The running time of this algorithm if $O(m(\log m)(\log^2 n))$.
2. The best known algorithm for when N has a reasonably small factor (say $N \approx 2^{1000}, p \approx 2^{100}$) is based on elliptic curves.
3. If we are allowed to use quantum computers, we can actually factorise integers in polynomial time with Shor's algorithm.