Part II – Number Theory

Based on lectures by Prof. A. Scholl

Notes taken by Bhavik Mehta

Michaelmas 2017

Contents

0 Introduction **2**

1 Euclid's algorithm and factoring **3**

2 Congruences **6**
2.1 Simultaneous Congruences 7
2.2 Polynomial Congruences 9

3 Quadratic residues **14**

4 Binary quadratic forms **23**

5 Distribution of the primes **33**
5.1 Elementary methods for primes 40
5.2 Divisibility of special numbers 40

6 Continued Fractions **44**
6.1 Continued Fraction algorithm 44
6.2 Rational Approximations 47

7 Primality testing and factorisation **51**
7.1 Factorisation 54

0 Introduction

Number theory is concerned with the (non-obvious, sometimes mysterious) properties of the integers, $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ and the rationals, $\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0\}$. It has been around for thousands of years, and has always been an experimental science where one can conduct experiments with numbers to spot their properties. Experimental data leads to conjectures which can turn out to be very hard to prove, for instance:

1. Congruent number problem: Let $N \geq 1$ be an integer of the form $8n + 5$, $8n + 6$ or $8n + 7$. Does there exist a right-angled triangle with sides of rational length, and area equal to N?

2. Twin prime conjecture: Does there exist infinitely many primes p such that $p + 2$ is also prime? Very recently, we know there are infinitely many primes p such that $\{p + 2, p + 4, \dots, p + 246\}$ contains a prime.

3. $\pi(x)$ refers to the prime counting function, the number of prime numbers $p \leq x$. The prime number theorem says that $\pi(x) \sim \mathrm{li}(x) \coloneqq \int_2^x \frac{dt}{\log t}$. It is not known whether or not $|\pi(x) - \mathrm{li}(x)| \leq \sqrt{x} \log(x)$, which is equivalent to the Riemann hypothesis - a statement about a certain complex analytic function.

Problem 1 follows from the Birch-Swinnerton-Dyer conjecture, related to algebraic geometry. Often these proofs can require sophisticated theorems, well beyond the statement of the problem.

1 Euclid's algorithm and factoring

Definition (Division algorithm)**.** Given $a, b \in \mathbb{Z}$, with $b > 0$, there are $q, r \in \mathbb{Z}$ with $0 \leq r < b$ and $a = bq + r$, that is, we can divide a by b to give a quotient q and remainder r.

Proof. Let $S = \{\, a - nb \mid n \in \mathbb{Z} \,\}$, which certainly contains some non-negative integers. Let r be the least of them, which exists by the well ordering property of the non-negative integers.

Claim $r < b$, since if not then $r - b \in S$ and $r - b \geq 0$, contradicting the choice of r. □

Notation. If $r = 0$ (that is, $a = bq$ for some $q \in \mathbb{Z}$), write $b \mid a$ (read as 'b divides a'), otherwise write $b \nmid a$.

Given $a_1, \ldots, a_n \in \mathbb{Z}$ not all zero, let

$$I = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_i \in \mathbb{Z}\}$$

We recognise this from GRM as the ideal generated by $\{a_1, \ldots, a_n\}$. Note if $a, b \in I$, for any choice of $l, m \in \mathbb{Z}$ then $la + mb \in I$.

Lemma 1.1. $I = d\mathbb{Z} = \{\lambda d \mid \lambda \in \mathbb{Z}\}$ for some $d \leq 1$, clearly unique.

Proof. As not all of a_i are 0, I contains some positive integer, let d be the least of them. So, $d \in I$, and hence $d\mathbb{Z} \subset I$.

On the other hand, for $a \in I$ the division algorithm gives us $a = qd + r$ with $0 \leq r < d$. But then $r = a - dq \in I$ so by minimality of d we have $r = 0$, and so $a \in d\mathbb{Z}$, giving $I \subset d\mathbb{Z}$ as required. □

Definition (Greatest common divisor)**.** $a_i \in I = d\mathbb{Z}$ so $d \mid a_i$. If in addition, we have that $\forall i$, $e \mid a_i$, then e divides every element of I, so $e \mid d$. Write $d = \gcd(a_1, \ldots, a_n) = (a_1, \ldots, a_n)$, the **greatest common divisor** (alternatively the highest common factor).

The study of **Diophantine equations** involves solving equations with integer solutions, and may have more variables than equations. The simplest case is linear in two variables, and can be solved easily.

Corollary. Let $a, b, c \in \mathbb{Z}$ with not both a, b equal to 0. Then we can find $x, y \in \mathbb{Z}$ such that $ax + by = c \Leftrightarrow (a, b) \mid c$.

The definition of the greatest common divisor given here is non-constructive, but Euclid's algorithm is an efficient way to compute it.

Euclid's algorithm: Assume $a > b > 0$. Apply successively the division algorithm:

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

for some k, so $r_k \mid r_{k-1}$

Claim $r_k = (a, b)$. Indeed,

$$\begin{aligned}(a, b) &= (a - q_1 b, b) = (b, r_1) \\ &= (r_1, r_2) = \cdots = (r_{k-1}, r_k) = r_k.\end{aligned}$$

Remark. By Lemma 1.1, $(a, b) = ra + sb$ for some integers r, s. Euclid's algorithm gives such r, s.

Example.

	x	y
$a = 34$	1	0
$b = 25$	0	1
$34 = 1 \cdot 25 + 9$	1	-1
$25 = 2 \cdot 9 + 7$	-2	3
$9 = 1 \cdot 7 + 2$	3	-4
$7 = 3 \cdot 2 + 1$	-11	15

so $\gcd(a, b) = -11a + 15b$, and the r_i are highlighted in red.

Recall that if $n > 1$ then n is **prime** if its only positive divisors are $\{1, n\}$, otherwise n is **composite**.

Lemma 1.2. Let p be prime, $a, b \in \mathbb{Z}$. Then $p \mid ab \implies p \mid a$ or $p \mid b$.

Proof. Suppose $p \mid ab$, $p \nmid a$. Then $\gcd(a, b) \neq p$, so it must be 1. So $\exists r, s \in \mathbb{Z}$ such that $ar + ps = 1$. Therefore, $b = (ab)r + p(bs)$, and hence $p \mid b$. □

This lets us prove the fundamental theorem of arithmetic.

Theorem (Fundamental theorem of arithmetic)**.** Every integer $n > 1$ can be written as a product of primes, and this representation is unique up to ordering.

Proof. Existence is trivial. Uniqueness: suppose $n = p_1 \dots p_r = q_1 \dots q_s$. $p_1 \mid n$, so p_1 divides some q_j. Hence $p_1 = q_j$ and so we can cancel p_1 and q_j from the relation, and repeat the process for $\frac{n}{p_1}$, eventually giving that the $\{p_1, \dots, p_r\}$ are the same as the $\{q_1, \dots, q_s\}$, up to ordering. □

If we know $a = \prod_{i=1}^{k} p_i^{\alpha_i}$, $b = \prod_{i=1}^{k} p_i^{\beta_i}$ for $\alpha_i, \beta_i \geq 0$ and p_i are distinct primes, then by uniqueness of prime factorisation,

$$(a, b) = \prod_{i=1}^{k} p_i^{\gamma_i}, \quad \gamma_i = \min(\alpha_i, \beta_i)$$

However if a, b are large, this is an inefficient way to compute GCDs.

Definition (Polynomial time)**.** An algorithm with input an integer $N > 0$ is **polynomial time** if $\exists b, c > 0$ for which the algorithm completes after less than $c(\log N)^b$ 'elementary operations'. Examples of elementary operations include adding or multiplying digits in some fixed base.

If there are k integer inputs, we require less than $c(\max_k(\log N_i))^b$ operations.

Example.

- Adding, multiplying integers (usual method)
- Computing GCDs by Euclid's algorithm
- Testing if N is prime (recent discovery, 2002)

Factoring

What about factoring N? The obvious method is trial division by integers $\leq \sqrt{N}$. If $N = pq$, then $p, q \sim \sqrt{N}$ this will take $\sqrt{N}$ divisions - asymptotically larger than any power of $\log N$. For instance, if N has 100 digits, and we can do 2^9 divisions every second, this will take around $10^{50}/2^9$ seconds, which is about 6×10^{39} years. However, Euclid's algorithm will compute the GCD of two such numbers in a few milliseconds.

However, there are better algorithms for factoring which we will see later, but so far no polynomial-time algorithm is known (important for security of encryption algorithms like RSA). These are practical for numbers with fewer than 200 digits (for a large computer - the record is 232 digits using thousands of computers and several months)

We will study the distribution of primes and the counting function later. For now,

Theorem (Euclid)**.** There are infinitely many primes.

Proof. It is enough to show that given N, there is a prime $p > N$. Let q be the largest prime $\leq N$, and set $M = (2 \times 3 \times 5 \times \cdots \times q) + 1$. If p is any prime factor of M, then $p \notin \{2, 3, \ldots, q\}$ so $p > N$. □

Remark. This is constructive, in that it gives a way to find a prime greater than any N, but is is not efficient. For instance, if $N = 1000$, M has over 400 digits.

Finding large primes: For reasonable size numbers (fewer than 1000 digits), it is reasonable to pick numbers at random and test for primality. For very large primes, there are special (faster) tests for primality of numbers of the form $N = 2^q - 1$, called Mersenne numbers. Using these, it has been shown that that $2^q - 1$ is prime when $q = 74207281$.

2 Congruences

Fix $n \geq 1$ (the modulus). Typically we will use $n > 1$.

Definition (Congruent)**.** $a \equiv b \pmod{n}$ iff $n \mid a - b$, and we say 'a is **congruent to** b **mod** n'

This defines an equivalence relation on $\mathbb{Z}$. Write $\mathbb{Z}/n\mathbb{Z}$ for the set of equivalence classes $\{a + n\mathbb{Z}\}$, where $a + n\mathbb{Z} = b + n\mathbb{Z} \iff a \equiv b \pmod{n}$. It is easy to see that the operations of addition and multiplication in $\{a + n\mathbb{Z}\}$ are well defined. (In other words, $n\mathbb{Z}$ is an ideal in the ring $\mathbb{Z}$, and $\mathbb{Z}/n\mathbb{Z}$ is the quotient ring.)

Lemma 2.1. Let $a \in \mathbb{Z}$. The following are equivalent:

i. $(a, n) = 1$

ii. $\exists b \in \mathbb{Z}$ with $ab \equiv 1 \pmod{n}$

iii. (The equivalence class of) a is a generator of the group $(\mathbb{Z}/n\mathbb{Z}, +)$.

Proof.

i. $\Rightarrow$ ii. If $(a, n) = 1$, $\exists b, c \in \mathbb{Z}$ with $ab + nc = 1$ so $ab \equiv 1 \pmod{n}$

ii. $\Rightarrow$ i. $ab \equiv 1 \pmod{n} \iff ab + kn = 1$, for some $k \in \mathbb{Z} \implies (a, n) = 1$

ii. $\Leftrightarrow$ iii. $ab \equiv 1 \pmod{n}$ for some $b \iff 1$ belongs to the subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by $a \iff$ the subgroup generated by a is $\mathbb{Z}/n\mathbb{Z}$

□

Notation. For $n > 1$, we write $(\mathbb{Z}/n\mathbb{Z})^*$ to denote the set of units (invertible elements) of $\mathbb{Z}/n\mathbb{Z}$.

By Lemma 2.1, this is the set of classes $a + n\mathbb{Z}$ where $(a, n) = 1$.

Definition (Euler φ-function)**.** We can then define the **Euler φ-function**:

$$\varphi(n) \coloneqq \#(\mathbb{Z}/n\mathbb{Z})^* = \#\left\{ a \in \mathbb{Z} \mid 1 \leq a \leq n,\ (a, n) = 1 \right\}.$$

Remark. For $n > 1$,

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} \text{ is a field} &\iff \text{every non-zero element has an inverse under } \times \\ &\iff n \text{ is prime} \\ &\iff \varphi(n) = n - 1 \end{aligned}$$

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

Proof. ($n > 1$) Apply Lagrange's theorem to the group $G = (\mathbb{Z}/n\mathbb{Z})^*$ which has order $\varphi(n)$. Then $a \in \mathbb{Z}$ with $(a, n) = 1$ defines an element of G whose order divides $\varphi(n)$. So $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

This has an important special case, called Fermat's Little Theorem.

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

Proof. Trivial if $p \mid a$. If not, $(a, p) = 1$ so $a^{\varphi(p)} \equiv 1 \pmod{p} \implies a^p \equiv a \pmod{p}$ □

Lemma 2.2. Let G be a cyclic group of order $n \geq 1$. Then

$$\begin{aligned}\varphi(n) &= \#\{\, g \in G \mid \text{order of } g \text{ is } n \,\} \\ &= \#\text{ of generators of } G\end{aligned}$$

Proof. We may assume $G = \mathbb{Z}/n\mathbb{Z}$, in which case this is just Lemma 2.1 □

2.1 Simultaneous Congruences

Example. We would like to find all $x \in \mathbb{Z}$ such that $x \equiv 7 \pmod{10}$ and $x \equiv 3 \pmod{13}$. One way might be to try $7, 17, 27, \ldots$ in turn.

A better way: suppose we have $u, v \in \mathbb{Z}$ such that

$$\begin{aligned} u &\equiv 1 \pmod{10} & \qquad v &\equiv 0 \pmod{10} \\ u &\equiv 0 \pmod{13} & \qquad v &\equiv 1 \pmod{13} \end{aligned}$$

Then $x = 7u + 3v$ is a solution.

To find u, v: $(10, 13) = 1$ so $\exists r, s$ with $10r + 13s = 1$, then setting $u = 13s$ and $v = 10r$ ensures the above congruences are satisfied. From the Euclidean algorithm, we see $r = 4$ and $s = -3$ work, so $u = -39$ and $v = 40$.

We can confirm $x = 7(-39) + 3(40) \equiv 107 \pmod{130}$ is a solution. In fact, the set of all solutions is $\{\, x \mid x \equiv 107 \pmod{130} \,\}$.

This is a special case of

Theorem (Chinese Remainder Theorem)**.** Let $m_1, \ldots, m_k$ be integers ≥ 1 with $(m_i, m_j) = 1$ if $i \neq j$ (they are pairwise coprime). Write $M = m_1 \cdots m_k$ for $k \geq 2$. Let $a_1, \ldots, a_k \in \mathbb{Z}$. Then there exists a solution $x \in \mathbb{Z}$ of

$$\left.\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}\right\} \qquad (*)$$

and x is unique mod M.

Remark. If x satisfies $(*)$, then so does $x + Mn$ for $n \in \mathbb{Z}$, so the solution set is just $x + M\mathbb{Z}$.

Proof.

- Uniqueness: If x, y satisfies $(*)$, then $m_i \mid (x - y)$ for every i. As no prime divides two of the m_i, it follows that $M = \prod m_i \mid (x - y)$, so $x \equiv y \pmod{M}$.
- Existence: Write $M_i = M/m_i = \prod_{j \neq i} m_j$. By the hypothesis, $(M_i, m_i) = 1$. So $\exists c_i \in \mathbb{Z}$ with $c_i M_i \equiv 1 \pmod{m_i}$. Obviously $c_i M_i \equiv 0 \pmod{m_j}$ $\forall j \neq i$. Let $x = \sum_{i=1}^{k} a_i c_i M_i$, then x satisfies $(*)$, as required. □

Note we find the c_i by Euclid's algorithm, so this is constructive.

Corollary. If $M = \prod_{i=1}^{k} m_i$, with m_i pairwise coprime, then

$$\varphi(M) = \varphi(m_1) \cdots \varphi(m_k)$$

Proof. $(a, M) = 1 \iff \forall i, (a, m_i) = 1$. So by the Chinese Remainder Theorem, we have a bijection

$$\{\, 1 \le x \le M \mid (x, M) = 1 \,\} \xleftrightarrow{\sim} \{\, (a_1, \dots, a_k) \mid 1 \le a_i \le m_i, (a_i, m_i) = 1 \,\}$$

So

$$\#\text{LHS} = \varphi(M) \ , \ \#\text{RHS} = \prod_i \varphi(m_i)$$

and thus they are equal. □

Algebraic aside: We can write this in terms of the rings $R_i = \mathbb{Z}/m_i\mathbb{Z}$.

Definition (Product ring)**.** The **product ring** is

$$R_1 \times \cdots \times R_k = \{\, (r_1, \dots, r_k) \mid r_i \in R_i \,\}$$

with $+, \times$ defined component-wise. This is a ring with 0 as the zero vector, and 1 as the vector of ones.

Theorem 2.3. Take $M = \prod m_i$, with m_i pairwise coprime. The map

$$\begin{aligned} \Theta : \mathbb{Z}/M\mathbb{Z} &\longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \\ a + M\mathbb{Z} &\longmapsto (a + m_1\mathbb{Z}, \dots, a + m_k\mathbb{Z}) \end{aligned}$$

is an isomorphism of rings.

Proof. $m_i \mid M \Rightarrow a + m_i\mathbb{Z}$ only depends on $a + M\mathbb{Z}$, so Θ is well-defined. It is a homomorphism (by definition of $+, \times$ in the product ring), and the Chinese Remainder Theorem implies that it is bijective. □

Definition (Multiplicative function)**.** A **multiplicative function** is a function $f : \mathbb{N} = \{1, 2, 3, \dots\} \to \mathbb{C}$ for which

$$(m, n) = 1 \implies f(mn) = f(m)f(n)$$

(This is the traditional terminology, although it is confusing we don't require $\forall m, n, f(mn) = f(m)f(n)$, which is sometimes called **totally multiplicative**.)

Example. Examples of multiplicative functions.

- $\varphi(n)$
- $\tau(n) = \#$ of positive divisors of n
- $\sigma(n) = \sum_{1 \le d \mid n} d$
- More generally $\sigma_k(n) = \sum_{1 \le d \mid n} d^k$, note $\sigma = \sigma_1, \tau = \sigma_0$

Lemma 2.4. Let f be a multiplicative function. Then so is g, defined by

$$g(n) = \sum_{d \mid n} f(d)$$

Proof. Let $(m,n)=1$. Then $\{\text{divisors } d \text{ of } mn\} = \{d = d_1 d_2 : d_1 \mid m, d_2 \mid n\}$.

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

Example. $f(n) = n^k$ (obviously multiplicative). Then $g(n) = \sigma_k(n)$. Later we will see how to recover f from g.

Theorem 2.5.

(i) p prime, $k \leq 1 \implies \varphi(p^k) = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$

(ii) For $n \geq 1$, $\varphi(n) = n \prod_{p \mid n}\left(1 - \frac{1}{p}\right)$ where the product is over primes.

(iii) $\sum_{d \mid n} \varphi(d) = n$

Proof.

(i) $\varphi(p^k) = \#\left\{\, 1 \leq a \leq p^k : p \nmid a \,\right\} = p^k - p^{k-1}$

(ii) Write

$$n = \prod_i p_i^{k_i}$$

with p_i distinct primes. Then,

$$\begin{aligned} \varphi(n) &= \prod_i \varphi(p_i^{k_i}) \\ &= \prod_i p_i^{k_i}\left(1 - \frac{1}{p_i}\right) \\ &= n \prod_i \left(1 - \frac{1}{p_i}\right) \end{aligned}$$

(iii) By Lemma 2.4, the left hand side is multiplicative. The right hand side is obviously multiplicative, so it is enough to prove for $n = p^k$.

$$\begin{aligned} \sum_{d \mid n} \varphi(d) &= \varphi(1) + \varphi(p) + \cdots + \varphi(p^k) \\ &= 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) \\ &= p^k. \end{aligned}$$

$\square$

2.2 Polynomial Congruences

We will take $R = \mathbb{Z}, \mathbb{Q}$ or $\mathbb{Z}/n\mathbb{Z}$ (or any commutative ring with 1) Recall $R[X]$ refers to polynomials in X taking coefficients from R, formally:

$$R[X] \coloneqq \{\, a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \mid n \geq 0,\ a_i \in R \,\}$$

Two polynomials are equal if their coefficients are the same. Importantly, a polynomial $f \in R[X]$ determines a function $R \to R$, given by $\alpha \mapsto f(\alpha) = \sum a_i \alpha^i$. It can happen that different polynomials give the same function.

Example. For p a prime and $R = \mathbb{Z}/p\mathbb{Z}$, consider $f(X) = X^p - X$. Then $\forall a \in R$, $f(a) = 0$ in $\mathbb{Z}/p\mathbb{Z}$ by Fermat's Little Theorem. So f and the zero polynomial determine the same function.

Multiplication and addition of polynomials is defined in the obvious way: for $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{i=0}^{n} b_i X_i$, we have

$$f + g = \sum_{i=0}^{n} (a_i + b_i) X^i$$

$$fg = \sum_{i=0}^{2n} \left(\sum_{j+k=i} a_j b_k \right) X^i$$

so $R[X]$ is a ring.

We also have a division algorithm for polynomials, where the measure of size is the degree.

Definition (Degree)**.** $\deg(f)$ is the largest i for which the coefficient of X^i is non-zero, and $\deg(f) = -\infty$ if f is the zero polynomial.

We also have $\deg(fg) \leq \deg(f) + \deg(g)$.

Definition (Divison algorithm for polynomials)**.** Let $f, g \in R[X]$. Assume that the leading coefficient of g is a unit in R (that is, has an inverse under multiplication) Then $\exists q, r \in R[X]$ with $\deg(r) < \deg(g)$ and $f = gq + r$.

Proof. Induction on $\deg f$. If $\deg f < \deg g$, then $q = 0$ and $r = f$ will do.

Otherwise $f = aX^m + \ldots$, $a \neq 0$, $g = bX^n + \ldots$, with $b = \frac{1}{c}$ invertible by assumption and $m \geq n$.

Then $f_1 = f - acX^{m-n} g \in R[X]$ has degree strictly less than m. So $f_1 = gq_1 + r$ say, $\deg(r) < \deg(g)$ and so $f = (q_1 + acX^{m-n})g + r$, as required. □

Corollary 2.6 (Remainder theorem)**.** Take $f \in R[X]$ and $\alpha \in R$. Then

$$f(X) = (X - \alpha) f_1(X) + f(\alpha)$$

Proof. Apply the division algorithm with $g = X - a$, so $f = (X - \alpha) f_1 + c$. c has degree less than 1, so must be in R. Now, evaluate both sides at $X = \alpha$, so $c = f(\alpha)$. □

In particular, if $f(\alpha) = 0$ then $f(X) = (X - \alpha) f_1(X)$. However in general a polynomial can have more roots than its degree - consider $f(X) = X^2 - 1$ with $R = \mathbb{Z}/8\mathbb{Z}$

Definition (Integral domain)**.** A nonzero ring R is an **integral domain** if $ab = 0$ implies $a = 0$ or $b = 0$.

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

Theorem 2.7. If R is an integral domain, and $f \in R[X]$ is a non-zero polynomial of degree $n \geq 0$, then f has $\leq n$ roots in R.

Corollary (Lagrange's Theorem)**.** Take p prime, $f \in \mathbb{Z}[X]$ of degree n, and f not divisible by p. Then the congruence $f(x) \equiv 0 \pmod{p}$ has $\leq n$ solutions mod p.

Proof. The $n = 0$ case is trivial. Suppose $n > 0$. If f has no roots in R, we have nothing to prove.

Otherwise $\exists \alpha \in R$, $f(\alpha) = 0$ so $f(X) = (X - \alpha) f_1(X)$, $f_1 \in R[X]$ with $\deg(f_1) = n - 1$. By induction, f_1 has $\leq n - 1$ roots in R. If β is a root of f, then $(\beta - \alpha) f_1(\beta) = 0$ so either $\beta = \alpha$ or $f_1(\beta) = 0$, as R is an integral domain. So, the roots of f are exactly α and the roots of f_1, so f has $\leq n$ roots. □

Example. Take p prime, and set

$$f(X) = X^{p-1} - 1 - \prod_{a=1}^{p-1} (X - a) \in \mathbb{Z}/p\mathbb{Z}[X]$$

Then, $\deg f \leq p - 2$. If $a = 1, \ldots, p - 1$ then $a^{p-1} \equiv 1 \pmod{p}$ so $f(a) = 0 \in \mathbb{Z}/p\mathbb{Z}$. So as f has $\geq p - 1$ roots mod p, it must be identically zero mod p. So $f(0)$ is zero mod p, and

$$-1 - \prod_{a=1}^{p-1} (-a) \equiv 0 \pmod{p}$$

giving us Wilson's Theorem: $(p - 1)! \equiv -1 \pmod{p}$.

The additive group $(\mathbb{Z}/n\mathbb{Z}, +)$ is cyclic. What about $((\mathbb{Z}/n\mathbb{Z})^*, \times)$?

Example. Consider $n = 7$, then we can check 3 is a generator of $(\mathbb{Z}/n\mathbb{Z})^*$ and hence the group is cyclic.

Theorem 2.8. If p is prime, then $G = (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p - 1$.

Proof. $\#G = p - 1 = \sum_{d|p-1} \varphi(d)$ by Theorem 2.5 part (iii).

Also, by Lagrange's Theorem in elementary group theory,

$$\#G = \sum_{d|p-1} \#\{\, g \in G \text{ of order d} \,\} = \sum_{d|p-1} N_d$$

Suppose G is not cyclic, so G has no element of order $p - 1$, then $N_{p-1} = 0 < \varphi(p - 1)$. As $\sum \varphi(d) = \sum N_d$, there exists some d for which $N_d > \varphi(d) > 0$. Let $\alpha \in G$ be an element of order d. Then $\langle \alpha \rangle \coloneqq \{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\} \subset G$ is a cyclic subgroup of order d so has exactly $\varphi(d)$ elements of order d by Lemma 2.2.

So $\exists \beta \notin \langle \alpha \rangle$ where β has order d. Then $1, \alpha, \alpha^{d-1}, \beta$ are $(d + 1)$ roots of the polynomial $X^d - 1$, contradicting Theorem 2.7. So, G must be cyclic. □

Definition (Primitive root)**.** If g is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ then g is said to be a **primitive root mod** p.

By Theorem 2.8, primitive roots exist.

Example. Take $p = 19$, and let d be the order of 2 inside $(\mathbb{Z}/19\mathbb{Z})^*$, then $d \mid p - 1 = 18$. We have $2^6 \equiv 7 \not\equiv 1 \pmod{19}$, so $d \nmid 6$. Similarly, $2^9 \equiv -1 \pmod{19}$ so $d \nmid 9$. Hence, $d = 18$ and 2 is a primitive root mod 19.

There are many unsolved problems about primitive roots:

1. Artin's Primitive Root conjecture:

   Fix a prime $g \geq 2$. Then there exist infinitely many p for which g is a primitive root mod p (say g is prime). Even the case $g = 2$ is unknown. From analytic number theory, it is known there are infinitely many p for which one of $2, 3, 5$ is a primitive root.

2. How large is the smallest primitive root mod p?

   We can show that this goes to ∞ as p grows. It is known that is is bounded above by $cp^{1/4+\epsilon}$ for any $\epsilon > 0$, but expected to be smaller (bounded by $c(\log p)^2$).

Now let's consider the more general case of $(\mathbb{Z}/p^n\mathbb{Z})^*$ for $n > 1$, and ask if it is cyclic. $(\mathbb{Z}/8\mathbb{Z})^* = \{\pm 1, \pm 3\}$, which all have order 1 or 2, so the group is not cyclic. If $n \geq 3$, the map $(\mathbb{Z}/2^n\mathbb{Z})^* \to (\mathbb{Z}/8\mathbb{Z})^*$ is surjective:

$$\forall n \geq 1, \quad (x, 8) = 1 \iff x \text{ odd} \iff (x, 2^n) = 1$$

So, $(\mathbb{Z}/2^n\mathbb{Z})^*$ is not cyclic for $n \geq 3$ since a generator would map to a generator of $(\mathbb{Z}/8\mathbb{Z})^*$.

Theorem 2.9. If $p > 2$ and $n \geq 1$ then $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic.

Proof. The proof is deferred until Page 13. □

Lemma 2.10. Take p an odd prime, and let $y \in \mathbb{Z}$ and $k \geq 1$. 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.

(i) We may as well assume (by replacing y with $y + pz$) that $x = 1 + p^k y$. Then,

$$\begin{aligned} x^p &= \sum_{j=0}^{p} \binom{p}{j} (p^k y)^j \\ &= 1 + p^{k+1} y + \sum_{j=2}^{p-1} \binom{p}{j} p^{kj} y^j + p^{p^k} y^p. \end{aligned}$$

For $2 \leq j \leq p-1$, we have $\binom{p}{j} \equiv 0 \pmod{p}$ and hence $\binom{p}{j} p^{kj} \equiv 0 \pmod{p^{2k+1}}$ and $2k+1 \geq k+2$. Since $p > 2$, we have $p^k \geq k+2$ so the last term is also $\equiv 0 \pmod{p^{k+2}}$, hence we are done.

(ii) Apply part (i) k times to $1 + py$. □

Lemma 2.11. If $g \in \mathbb{Z}$, $(g, p) = 1$, g is a primitive root mod p, and $g^{p-1} \not\equiv 1 \pmod{p^2}$, then g is a generator of $(\mathbb{Z}/p^n\mathbb{Z})^* = G$.

Proof. Let d be the order of g in G. We know $d \mid \#G = p^{n-1}(p-1)$, so if g is not a generator, one of the following two cases must hold:

(i) $d \mid p^{n-2}(p-1)$, so $g^{p^{n-2}(p-1)} \equiv 1 \pmod{p^n}$.

(ii) $d = p^{n-1}e$, with $1 \leq e < p-1$ and $e \mid p-1$, and so $g^{p^{n-1}e} \equiv 1 \pmod{p^n}$.

Deal with these cases in turn:

(i) Let $x = g^{p-1} = 1 + py$ with $y \not\equiv 0 \pmod{p}$, because $g^{p-1} \not\equiv 1 \pmod{p^2}$. Then by Lemma 2.10 (ii), we have $x^{p^{n-2}} \equiv 1 + p^{n-1}y \pmod{p^n}$, so $g^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n}$.

(ii) $g^{p^{n-1}e} \equiv g^e \pmod{p}$ by Euler-Fermat, and this is not congruent to $1 \pmod{p}$ as g is a primitive root mod p.

So neither (i) nor (ii) can hold, and hence g has order $p^{n-1}(p-1)$. □

We can return and prove Theorem 2.9.

Proof of Theorem 2.9. Let $g \in \mathbb{Z}$ be a primitive root mod p. If $g^{p-1} \not\equiv 1 \pmod{p^2}$, then by Lemma 2.11, g generates $(\mathbb{Z}/p^n\mathbb{Z})^*$. If not, $g^p \equiv g \pmod{p^2}$. Let $g_1 = g(1+p)$. Then, $g_1^p = g^p(1+p)^p$ and $(1+p)^p \equiv 1 \pmod{p^2}$ by Lemma 2.10.

So, $g_1^p \equiv g^p \pmod{p^2} \equiv g \pmod{p^2} \not\equiv g_1 \pmod{p^2}$, so by Lemma 2.11, g_1 generates $(\mathbb{Z}/p^n\mathbb{Z})^*$. □

Remark.

1. Our proof gives an easy way to find a generator for $(\mathbb{Z}/p^n\mathbb{Z})^*$, independent of $n \geq 2$.
2. What happens when $p = 2$? Lemma 2.10(i) fails to hold for $p = 2$, $k = 1$: $(1+2)^2 \equiv 1 \pmod{8}$. It does hold for $p = 2$ and $k \geq 2$ however. Part (ii) becomes $(1+4)^{k-1} \equiv 1 + 2^{k+1} \pmod{2^{k+2}}$. We can then show (following the argument for p odd), that $(\mathbb{Z}/2^n\mathbb{Z})^*$ for $n \geq 3$ is generated by -1 and 5 which have orders 2 and 2^{n-2} respectively. So, we have that
$$(\mathbb{Z}/2^n\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$$
3. If $N = \prod_{1 \leq i \leq r} p_i^{k_i}$, then
$$(\mathbb{Z}/N\mathbb{Z})^* \cong (\mathbb{Z}/{p_1}^{k_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/{p_r}^{k_r}\mathbb{Z})^*$$
by the Chinese Remainder Theorem.

3 Quadratic residues

Take $p > 2$ an odd prime. If $a \in \mathbb{Z}$, we know $x^2 \equiv a \pmod{p}$ has ≤ 2 solutions mod p.

For $a \equiv 0 \pmod{p}$, then there is one solution, $x \equiv 0 \pmod{p}$. For $a \not\equiv 0 \pmod{p}$, if x is a solution then so is $-x$, and $-x \equiv x \pmod{p} \Leftrightarrow 2x \equiv 0 \pmod{p}$ but $a \not\equiv 0 \Rightarrow x \not\equiv 0 \pmod{p}$ so we have either 0 or 2 solutions.

Definition (Quadratic residue)**.** $a \equiv 0 \pmod{p}$ is a **quadratic residue** mod p if $x^2 \equiv a \pmod{p}$ is soluble, and a **quadratic non-residue** if not.

So a is a quadratic residue mod p iff its class in $(\mathbb{Z}/p\mathbb{Z})^*$ is a square.

Example. Computing squares mod 7,

x	1	2	3	4	5	6
x^2	1	4	2	2	4	1

the quadratic residues mod 7 are $\{1, 2, 4\}$.

Lemma 3.1. Let p be an odd prime. There are exactly $\frac{p-1}{2}$ quadratic residues mod p.

Proof 1. Consider

$$\begin{aligned} \sigma : (\mathbb{Z}/p\mathbb{Z})^* &\longrightarrow (\mathbb{Z}/p\mathbb{Z})^* \\ x &\longmapsto x^2 \pmod{p} \end{aligned}$$

Then

$$\begin{aligned} & \sigma(x) = \sigma(y) \\ \iff & x^2 \equiv y^2 \pmod{p} \\ \iff & (x-y)(x+y) \equiv 0 \pmod{p} \\ \iff & x \equiv \pm y \pmod{p} \end{aligned}$$

Since p is odd, if $(x, p) = 1$ then $x \not\equiv -x \pmod{p}$. So, σ is 2-to-1, hence the image of σ has $\frac{p-1}{2}$ elements. □

Proof 2. Let g be a primitive root mod p. Then $(\mathbb{Z}/p\mathbb{Z})^* = \{1, g, g^2, \ldots, g^{p-2}\}$ as $g^{p-1} = 1$. So,

$$\begin{aligned} \{\, x^2 \mid x \in (\mathbb{Z}/p\mathbb{Z})^* \,\} &= \{1, g^2, g^4, \ldots, g^{p-3}, g^{p-1}, g^{p+1}, \ldots, g^{2p-4}\} \\ &= \{1, g^2, g^4, \ldots, g^{p-3}\} \end{aligned}$$

since $g^{p-1} = 1$ and $g^{p+1} = g^2$, and so on, hence there are $\frac{p-1}{2}$ elements. □

Definition (Legendre symbol)**.** The **Legendre symbol** of a mod p (for p an odd prime, $a \in \mathbb{Z}$) is

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

Lemma (Euler's Criterion)**.**

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

Remark. $\left(\frac{a}{p}\right) \in \{0, \pm 1\}$ which is a set of 3 distinct integers mod p as $p > 2$. So the congruence in the lemma determines $\left(\frac{a}{p}\right)$ completely.

Proof. If $p \mid a$, obvious. Suppose $(a, p) = 1$. Then $a^{p-1} = \left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}$. Hence $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. If $a \equiv x^2 \pmod{p}$, then $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv +1 \pmod{p}$. By Lemma 3.1, this gives $\frac{p-1}{2}$ solutions of $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. So there are no more solutions, i.e. if $\left(\frac{a}{p}\right) = -1$, then $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Corollary 3.2. Take $a, b \in \mathbb{Z}$ where p is an odd prime. Then

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

Proof.

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

By the previous remark, we have $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

Remark. We have the following equivalent statements

- The map

$$(\mathbb{Z}/p\mathbb{Z})^* \longrightarrow \{\pm 1\}$$

$$a \longmapsto \left(\frac{a}{p}\right)$$

  is a homomorphism of groups.

- The product of residues is a residue; the product of a residue and non-residue is a non-residue, and the product of non-residues is a residue.

Another consequence of Euler's Criterion allows efficient computation of $\left(\frac{a}{p}\right)$ because there is a polynomial time algorithm to compute $a^n \pmod{N}$.

- write $n = n_0 + 2n_1 + 4n_2 + \cdots + 2^k n_k$ in binary, $n_i \in \{0, 1\}$
- compute a^2, $a^4 = (a^2)^2$, $a^8 = (a^4)^2, \ldots, a^{2^k} \pmod{N}$.
- $a^n \equiv \prod_{i:n_i=1} a^{2^i} \pmod{N}$

Corollary 3.3. For p an odd prime,

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

Proof. By Euler's criterion, if $p = 4k + l$, with $l = 1$ or 3,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2k+\frac{l-1}{2}} = \begin{cases} +1 & l = 1 \\ -1 & l = 3. \end{cases}$$ □

What about $\left(\frac{2}{p}\right)$? So what is $2^{\frac{p-1}{2}} \pmod p$? Recall the proof of Fermat's Little Theorem, and imitate this using $\left(\frac{p-1}{2}\right)!$ instead. This will prove

Lemma (Gauss's Lemma)**.** Take p an odd prime and $(a, p) = 1$. Then $\left(\frac{a}{p}\right) = (-1)^\mu$ where μ is the number of $j \in \{1, \ldots, \frac{p-1}{2}\}$ such that $aj \equiv k \pmod p$ where $\frac{p+1}{2} \leq k \leq p - 1$.

Proof. $1 \leq j \leq \frac{p-1}{2}$. Write $aj \equiv \epsilon_j c_j \pmod p$ with $1 \leq c_j \leq \frac{p-1}{2}$ and $\epsilon_j \in \{\pm 1\}$ (by reducing $aj \bmod p$ into the interval $(-\frac{p}{2}, \frac{p}{2})$).

Now claim that if $j \neq k$ with $1 \leq j, k \leq \frac{p-1}{2}$ then $c_j \neq c_k$. Indeed if $c_j = c_k$ then $\epsilon_j aj \equiv \epsilon_k ak \pmod p$, that is, $j \equiv \pm k \pmod p$. As $1 \leq j, k \leq \frac{p-1}{2}$, $j + k \not\equiv 0 \pmod p$ so $j = k$. So, $\left\{c_1, \ldots, c_{\frac{p-1}{2}}\right\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ in some order.

Now,

$$\mu = \#\left\{ j \in \left\{1, \ldots, \tfrac{p-1}{2}\right\} \;\middle|\; aj \equiv k \bmod p, \frac{p+1}{2} \leq k \leq p-1 \right\} = \#\{\, j \mid \epsilon_j = -1 \,\}$$

So,

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

This gives

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

Example. Take the (trivial) special case of $a = -1$, then $-j \in (-\frac{p}{2}, 0)$ so $\epsilon_j = -1$ and $c_j = j$ for any j. So, $\mu = \frac{p-1}{2}$ and $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Now consider the case of $n = 2$. Then

$$\{\, 2j \mid 1 \leq j \leq \tfrac{p-1}{2} \,\} = \{2, 4, \ldots, p-3, p-1\}$$

If $0 < j < \frac{p}{4}$ then $2j \in \{1, \ldots, \frac{p-1}{2}\}$ while if $\frac{p}{4} < j < \frac{p}{2}$ then $\frac{p}{2} < 2j < p$. So,

$$\begin{aligned} \mu &= \#\left\{ j \in \mathbb{Z} \;\middle|\; \frac{p}{4} < j < \frac{q}{2} \right\} \\ &= \left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor \end{aligned}$$

Split into cases:

$$\begin{array}{lll} p = 8k+1 & \implies & \mu = 4k - 2k = 2k & \implies (-1)^\mu = 1 \\ p = 8k+3 & \implies & \mu = (4k+1) - 2k = 2k+1 & \implies (-1)^\mu = -1 \\ p = 8k+5 & \implies & \mu = (4k+2) - (2k+1) = 2k+1 & \implies (-1)^\mu = -1 \\ p = 8k+7 & \implies & \mu = (4k+3) - (2k+1) = 2k+2 & \implies (-1)^\mu = 1 \end{array}$$

Note that $8 \mid p^2 - 1$ and that $16 \mid p^2 - 1 \iff p = 8k \pm 1$, both easy to check.

Corollary 3.4.

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases} = (-1)^{\frac{p^2-1}{8}}$$

What about $a = 3, 5, \ldots$? For $p > 3$, consider $\{\, 3j \mid 1 \le j \le \frac{p-1}{2} \,\}$.

$$0 < j < \tfrac{p}{6} \implies 0 < 3j < \tfrac{p}{2}$$

$$\tfrac{p}{6} < j < \tfrac{p}{3} \implies \tfrac{p}{2} < 3j < p$$

$$\tfrac{p}{3} < j < \tfrac{p}{2} \implies 0 < 3j - p < \tfrac{p}{2}$$

So, $\mu = \#\{\, j \mid \frac{p}{6} < j < \frac{p}{3} \,\}$ which we can work out from looking at p mod 12.

For general $1 \le a \le p-1$, look at $\{\, aj \mid 1 \le j \le \frac{p-1}{2} \,\}$. Then for $k \in \mathbb{Z}$,

$$kp < aj < \left(k + \frac{1}{2}\right) p \implies 0 < aj - kp < \frac{p}{2} \qquad \text{does not contribute to } \mu$$

$$\left(k - \frac{1}{2}\right) p < aj < kp \implies -\frac{p}{2} < aj - kp < 0 \qquad \text{contributes to } \mu$$

So

$$\mu = \sum_{k \in \mathbb{Z}} \# \left\{ j \;\middle|\; 1 \le j \le \frac{p-1}{2}, \left(k - \frac{1}{2}\right) \frac{p}{a} < j < \frac{kp}{a} \right\},$$

i.e. $-\frac{p}{2} < aj - kp < 0$. Note also that $0 < k < \frac{1}{2} + \frac{aj}{p} < \frac{a+1}{2}$.

Theorem (Quadratic Reciprocity)**.** For (p, q) distinct odd primes,

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

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

Example.

(i) $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$, but

$$(-1)^{\frac{p-1}{2}} = \begin{cases} +1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$$

$$\left(\frac{p}{3}\right) = \begin{cases} +1 & p \equiv 1 \pmod 3 \\ -1 & p \equiv 2 \pmod 3 \end{cases}$$

$$\therefore \left(\frac{3}{p}\right) = \begin{cases} +1 & p \equiv \pm 1 \pmod{12} \\ -1 & p \equiv \pm 5 \pmod{12} \end{cases}$$

(ii)

$$\left(\frac{19}{73}\right) = \left(\frac{73}{19}\right) = \left(\frac{16}{19}\right) = \left(\frac{4^2}{19}\right) = 1$$

(iii)

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

since $17 \equiv 5 \pmod{12}$.

Proof of Quadratic Reciprocity. By the previous calculation from Gauss' Lemma, $\left(\frac{q}{p}\right) = (-1)^{\mu}$ where

$$\mu = \#\left\{ (j,k) \in S \;\middle|\; 0 < kp - jq < \frac{p}{2} \right\}$$

and

$$S = \left\{ (j,k) \;\middle|\; 1 \leq j \leq \frac{p-1}{2}, 1 \leq k \leq \frac{q-1}{2} \right\}$$

By symmetry, $\left(\frac{p}{q}\right) = (-1)^{\nu}$ where

$$\nu = \#\left\{ (j,k) \in S \;\middle|\; 0 < jp - kq < \frac{p}{2} \right\}$$

Now, $\#S = \frac{p-1}{2}\frac{q-1}{2} = \mu + \nu + \#A + \#B$ where

$$A = \left\{ (j,k) \in S \;\middle|\; kp - jq > \frac{p}{2} \right\}$$
$$B = \left\{ (j,k) \in S \;\middle|\; jp - kq > \frac{p}{2} \right\}$$

If $(j,k) \in S$, write $j' = \frac{p+1}{2} - j$, $k' = \frac{q+1}{2} - k$. Then $(j',k') \in S$, and

$$j'q - k'p = \left(\frac{p+1}{2} - j\right)q - \left(\frac{q+1}{2} - k\right)p = \left(kp - jq - \frac{p}{2}\right) + \frac{q}{2}$$

So $(j,k) \in A \iff (j',k') \in B$, so $\#A = \#B$. Hence $\frac{p-1}{2}\frac{q-1}{2} = \mu + \nu + 2\#A$ and

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{u+v} = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right). \qquad \square$$

Example.

$$\begin{aligned}
\left(\frac{7411}{9283}\right) &= -\left(\frac{9283}{7411}\right) \\
&= -\left(\frac{1872}{7411}\right) \\
&= -\left(\frac{2^4 \cdot 3^2 \cdot 13}{7411}\right) \\
&= -\left(\frac{13}{7411}\right) \\
&= -\left(\frac{7411}{13}\right) \\
&= -\left(\frac{1}{13}\right) = -1
\end{aligned}$$

The problem here is that we needed to know that 7411 was prime and factor 1872. To avoid this, we will generalise the Legendre symbol to the Jacobi symbol.

Definition (Jacobi symbol)**.** Let $n \geq 1$ be odd, and $n = p_1 \cdots p_k$ with p_i primes, not necessarily distinct. The **Jacobi symbol** is

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{k} \left(\frac{a}{p_j}\right) \quad \text{for } a \in \mathbb{Z}$$

Note if $(a, n) > 1$ then $\left(\frac{a}{n}\right) = 0$, and if $n = 1$ then $\left(\frac{a}{1}\right) = 1$.

Proposition 3.5.

(i)
$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right) \text{ if } a \equiv b \pmod{n}$$

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

(iii)
$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

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

Proof.

(i)
$$a \equiv b \pmod{n} \implies \forall j, a \equiv b \pmod{p_j} \implies \forall j, \left(\frac{a}{p_j}\right) = \left(\frac{b}{p_j}\right)$$

(ii)
$$\forall j, \left(\frac{ab}{p_j}\right) = \left(\frac{a}{p_j}\right)\left(\frac{b}{p_j}\right)$$

This proves the first equation, while the second follows by definition.

(iii) This is true if n is prime, so by part (ii) it is enough to show that if $m, n \geq 1$ are odd then
$$(-1)^{\frac{m-1}{2}} \cdot (-1)^{\frac{n-1}{2}} = (-1)^{\frac{mn-1}{2}}.$$
Indeed, $(m-1)(n-1) \equiv 0 \pmod 4$, so $mn - 1 \equiv m + n - 2 \pmod 4$ and hence
$$\frac{mn-1}{2} \equiv \frac{m-1}{2} + \frac{n-1}{2} \pmod 2$$

(iv) Similarly to (iii), only need to show that for $m, n \geq 1$ odd
$$(-1)^{\frac{m-1}{2}} \cdot (-1)^{\frac{n-1}{2}} = (-1)^{\frac{mn-1}{2}}.$$
Indeed, $(m^2-1)(n^2-1) \equiv 0 \pmod{16}$ so $m^2n^2 - 1 \equiv m^2 + n^2 - 2 \pmod{16}$, hence
$$\frac{m^2n^2-1}{8} \equiv \frac{m^2-1}{8} + \frac{n^2-1}{8} \pmod 2. \qquad \square$$

Theorem 3.6 (Quadratic Reciprocity for Jacobi symbol)**.** Let $m, n \geq 1$ odd. Then

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

and if $(m, n) = 1$,

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

Proof. If $(m, n) > 1$, trivial since both sides are 0.

Assume that $(m, n) = 1$, with

$$m = \prod_{i=1}^{k} p_i, \; n = \prod_{j=1}^{l} q_j \quad \text{no } p_i = q_j$$

Let

$$r = \#\{\, i \mid p_i \equiv 3 \bmod 4 \,\}$$
$$s = \#\{\, j \mid q_j \equiv 3 \bmod 4 \,\}$$

(rest of the proof coming soon) □

For p prime and $(a, p) = 1$, $\left(\frac{a}{p}\right) = 1 \iff a$ is a square mod p. Generalising to the Jacobi symbol, for $n \geq 1$ odd and $(a, n) = 1$, if $a \equiv x^2 \pmod{n}$, then

$$\left(\frac{a}{n}\right) = \left(\frac{x^2}{n}\right) = \left(\frac{x}{n}\right)^2 = +1$$

but the converse does not hold! For instance

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = +1.$$

But 2 is not a square mod 15 as it is not a square mod 3 or mod 5.

Let $n = pq$, $p \neq q$ odd primes. Then by the CRT for $(a, pq) = 1$,

$$a \text{ is square mod } pq \iff a \text{ is a square mod } p \text{ and mod } q \iff \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$$

but of course

$$\left(\frac{a}{pq}\right) = 1 \iff \text{either} \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = +1$$
$$\text{or} \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = +1$$

If we know $\left(\frac{a}{pq}\right) = 1$, to determine whether or not a is a square mod pq, it is at least plausible that we need to know p and q, i.e. we need to factor n. (This is generally believed to be true - there are cryptographic protocols which rely on the difficulty of finding out whether a is a square mod $pq = n$, without knowing the factorisation of n.)

In computing Legendre symbols, need to factor the numerator to apply Quadratic Reciprocity. Using Theorem 3.6, this can be avoided. For instance,

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

where the fact that $33 \equiv 1 \pmod 4$ was used.

At worst, we have to take out factors of 2 (since Quadratic Reciprocity requires m, n odd):

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

So, it is very similar to Euclid's algorithm.

Are there higher reciprocity laws?

- Higher powers, for instance cubes mod p:

  If $p \equiv 2 \pmod 3$ then $3 \nmid p-1$, and we can easily see that everything is a cube mod p, since $x \mapsto x^3$ is a bijection $(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$.

  For $p \equiv 1 \pmod 3$, we can define a 'cubic Legendre symbol' taking values in $\{0\} \cup \{1, \omega, \omega^2\}$ where ω is a cube root of unity. There is a cubic reciprocity law. A big success of 19$^{\text{th}}$ century number theory was a proof of a reciprocity law for n^{th} powers, for any $n \geq 2$.

- A highlight of the (early) 20$^{\text{th}}$ century: Recall that for p odd,

$$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4 \iff p = x^2 + y^2 \text{ for some } x, y \in \mathbb{Z}$$
$$\iff p = (x+iy)(x-iy) \in \mathbb{Z}[i]$$

  This was hugely generalised to Artin's Reciprocity Law (in Algebraic Number Theory), and tells us how primes factor in more general number fields.

Another proof of infinitude of $p \equiv 3 \pmod 4$.

$$\left(\frac{-1}{n}\right) = \begin{cases} 0 & n \text{ even} \\ 1 & n \equiv 1 \pmod 4 \\ -1 & n \equiv 3 \pmod 4 \end{cases}$$

and we know

$$\left(\frac{-1}{n}\right) = \prod_i \left(\frac{-1}{p_i}\right) \text{ if } n = \prod_i p_i$$

The series

$$\sum_{n \geq 1} \left(\frac{-1}{n}\right)\frac{1}{n} = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \cdots$$

is convergent as it is an alternating series.

Suppose $p \equiv 3 \pmod 4$. Then

$$\begin{aligned}\left(1+\frac{1}{p}\right)\sum_{n\geq 1}\left(\frac{-1}{n}\right)\frac{1}{n} &= \sum_{n\geq 1}\left(\frac{-1}{n}\right)\frac{1}{n} + \sum_{m\geq 1}\left(\frac{-1}{m}\right)\frac{1}{mp} \\ &= \sum_{n\geq 1}\left(\frac{-1}{n}\right)\frac{1}{n} - \sum_{m\geq 1}\left(\frac{-1}{mp}\right)\frac{1}{mp} \\ &= \sum_{\substack{(n,p)=1 \\ n\geq 1}}\left(\frac{-1}{n}\right)\frac{1}{n}\end{aligned}$$

must also be convergent.

If there are only a finite set $\{p_1, \ldots, p_k\}$ of primes $\equiv 3 \pmod 4$, then

$$\left(1+\frac{1}{p_1}\right)\left(1+\frac{1}{p_2}\right)\cdots\left(1+\frac{1}{p_k}\right)\sum_{n\geq 1}\left(\frac{-1}{n}\right)\frac{1}{n} = \sum_{(n,p_1\cdots p_k)=1}\left(\frac{-1}{n}\right)\frac{1}{n} \qquad (*)$$

is also convergent. But $(n, p_1 \ldots p_k) = 1$ means that every odd prime dividing n is $\equiv 1 \pmod 4$ so

$$\left(\frac{-1}{n}\right) = \begin{cases} 0 & n \text{ even} \\ 1 & n \text{ odd} \end{cases}$$

$$\implies (*) = \sum_{(n,2p_1\cdots p_k)=1}\frac{1}{n}$$

but this is divergent. □

4 Binary quadratic forms

Motivating problem: Which $n \geq 1$ can be written as a sum of 2 integer squares?

Theorem 4.1. Take $N \geq 1$ an integer. Then N is a sum of two integer squares $\iff$ every prime factor $p \equiv 3 \pmod 4$ if N divides it to an even power.

Proof. ($\Rightarrow$) Suppose $N = x^2 + y^2$. Let $p \mid N$, $p \equiv 3 \pmod 4$. Then $x^2 \equiv -y^2 \pmod p$, so $x \equiv 0 \equiv y \pmod p$, since otherwise $\exists z \in \mathbb{Z}$ with $yz \equiv 1 \pmod p$ and $(xz)^2 \equiv -1 \pmod p$, but $\left(\frac{-1}{p}\right) = -1$. So $p^2 \mid N$ and $N/p^2 = (x/p)^2 + (y/p)^2$, then repeat until no prime factor $p \equiv 3 \pmod 4$ remains.

($\Leftarrow$) Write $N = M^2 N_1$, where N_1 is a product of distinct primes, each either 2 or $\equiv 1 \pmod 4$. It suffices to show $N_1 = x^2 + y^2$, since then $N = (Mx)^2 + (My)^2$.

As $(x^2 + y^2)(z^2 + t^2) = (xz - yt)^2 + (xt + yz)^2$ and $2 = 1^2 + 1^2$, it's enough to show if $p \equiv 1 \pmod 4$ then $p = x^2 + y^2$, which is done later (in lecture 11). □

There are similar results (Euler) for $x^2 + 2y^2$ and $x^2 + 3y^2$. However, $x^2 + 6y^2$ is complicated, we'll see why.

The general problem is to consider **binary quadratic forms** with integer coefficients

$$f(x, y) = ax^2 + bxy + cy^2 \quad a, b, c \in \mathbb{Z}$$

and ask what are possible sets $\{ f(x, y) \mid x, y \in \mathbb{Z} \}$?

Definition (Represent)**.** Say f **represents** $n \in \mathbb{Z}$ if $\exists x, y \in \mathbb{Z}$ with $f(x, y) = n$.

Definition (BQF)**.** A **BQF** is a binary quadratic form with coefficients in $\mathbb{Z}$.

We use the convenient shorthand (a, b, c) for the form $f = ax^2 + bxy + cy^2$. f can be written in matrix form:

$$ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Example.

- $f(x, y) = x^2 + y^2$ or $(1, 0, 1)$ has matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- $g(x, y) = 4x^2 + 12xy + 10y^2$ or $(4, 12, 10)$ has matrix $\begin{pmatrix} 4 & 6 \\ 6 & 10 \end{pmatrix}$.

Note $g(x, y) = (2x + 3y)^2 + y^2 = X^2 + Y^2 = f(X, Y)$, so f, g are related by an integer change of variables. But they don't represent the same set of integers - g only represents even integers.

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

Definition (Unimodular substitution)**.**

(1) A **unimodular substitution** is one of the form

$$X = \alpha x + \gamma y, \quad Y = \beta x + \delta y, \quad \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \quad \alpha\delta - \beta\gamma = 1$$
$$\text{so } \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = A^T \begin{pmatrix} x \\ y \end{pmatrix}, \quad A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

(2) BQFs f, g are **equivalent** if $f(X, Y) = g(x, y)$ for a unimodular substitution.

Remark.

(1) As A^{-1} has integer entries, if f, g are equivalent then they represent the same integers.

(2) (Exercise) Equivalence of BQFs is an equivalence relation

More formally,

$$\left\{ A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \;\middle|\; \alpha, \beta, \gamma, \delta \in \mathbb{Z},\ \alpha\delta - \gamma\beta = 1 \right\} =: \mathrm{SL}_2(\mathbb{Z})$$

is a group under matrix multiplication ($\det A = 1 \implies A^{-1} \in \mathrm{SL}_2(\mathbb{Z})$) which acts on the set of BQFs by

$$A : f(x, y) \longmapsto f(\alpha x + \gamma y, \beta x + \delta y)$$

and the equivalence classes of BQFs are the orbits of this action.

We can check this is a group action:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \implies Af = f$$

We must also check $(AB)f = (A(Bf))$. If $f = (a, b, c)$, $g = Af = (a', b', c')$ for $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ then

$$\begin{aligned} g(x, y) = f(X, Y) &= \begin{pmatrix} X & Y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} c & \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \\ &= \begin{pmatrix} x & y \end{pmatrix} A \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} A^T \begin{pmatrix} x \\ y \end{pmatrix} \end{aligned}$$

and

$$A \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} A^T = \begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix} \tag{$*$}$$

So to see that $A(Bf) = (AB)f$, write in matrix form

$$A \left[B \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} B^T \right] A^T = (AB) \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} B^T A^T$$

and $B^T A^T = (AB)^T$.

Definition (Discriminant)**.** The **discriminant** of $f = ax^2 + bxy + cy^2$ is $\mathrm{disc}(f) = b^2 - 4ac$. Observe $\mathrm{disc}(f) = -4 \times \det \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$.

Example.

$$\begin{aligned} \text{disc}(1,0,1) &= -4 \\ \text{disc}(4,12,10) &= -16 \end{aligned}$$

Lemma 4.2. Equivalent forms have the same discriminant (so the discriminant is an invariant of BQFs under equivalence).

Proof. Take identity $(*)$:

$$\begin{aligned} \begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c \end{pmatrix} &= A \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} A^T \\ \implies \text{disc}(a',b',c') &= \text{disc}(a,b,c) \det A \det A^T \\ &= \text{disc}(a,b,c) \end{aligned}$$

□

Remark. The converse is false: forms of the same discriminant need not be equivalent:

$$f = (1,0,6) = x^2 + 6y^2,\ g = (2,0,3) = 2x^2 + 3y^2$$

and $\text{disc}(f) = -24 = \text{disc}(g)$, but f represents 1 and g doesn't.

Lemma 4.3. $\exists$ BQF f with $\text{disc}(f) = d \iff d \equiv 0 \text{ or } 1 \pmod 4$.

Proof. $(\Rightarrow)$ $d = \text{disc}(a,b,c) = b^2 - 4ac \equiv b^2 \pmod 4 \implies d \equiv 0 \text{ or } 1 \pmod 4$

$(\Leftarrow)$ If $d \equiv 0 \pmod 4$ then $\text{disc}(1,0,-\frac{d}{4}) = d$ and if $d \equiv 1 \pmod 4$ then $\text{disc}(1,1,\frac{1-d}{4}) = d$.

□

Definition. A real quadratic form

$$f(\mathbf{x}) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j \quad (a_{ij} \in \mathbb{R})$$

is

- **positive definite** if $\forall x \in \mathbb{R}^n,\ x \neq 0 \Rightarrow f(\mathbf{x}) > 0$
- **negative definite** if $\forall x \in \mathbb{R}^n,\ x \neq 0 \Rightarrow f(\mathbf{x}) < 0$
- **indefinite** if $\exists \mathbf{x}, \mathbf{x'} \in \mathbb{R}^n$ with $f(\mathbf{x}) > 0 > f(\mathbf{x'})$

Consider the case $n = 2$:

Lemma 4.4. Take $f = (a,b,c)$ a BQF with $d = b^2 - 4ac$.

(i) $d < 0,\ a > 0 \implies f$ is positive definite

(ii) $d < 0,\ a < 0 \implies f$ is negative definite

(iii) $d > 0 \implies f$ is indefinite

(iv) $d = 0 \implies f = l(mx + ny)^2 \quad l,m,n \in \mathbb{Z}$

Proof.

(i),(ii) $d < 0$, so $ac > 0$ and a, c have the same sign.

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

so $\forall x, y \in \mathbb{R}$, $4af(x,y) \geq 0$ (as $d < 0$) with equality if and only if $x = y = 0$. f is positive definite if $a > 0$ and negative definite if $a < 0$.

(iii) Assume $d > 0$ and $a > 0$. Consider $f(x,1) = ax^2 + bx + c = a(x-\alpha)(x-\beta)$ with real $\alpha < \beta$ and

$$\alpha, \beta = \frac{-b \pm \sqrt{d}}{2a}$$

If $\frac{r}{s} \in \mathbb{Q}$,

$$f(r,s) = s^2 f\left(\frac{r}{s}, 1\right) = as^2\left(\frac{r}{s} - \alpha\right)\left(\frac{r}{s} - \beta\right)$$

$$\text{so for} \frac{r}{s} > \beta \qquad\qquad f(r,s) > 0$$

$$\alpha < \frac{r'}{s'} < \beta \qquad\qquad f(r',s') < 0$$

so f is indefinite. Indeed $\exists$ integer pairs $(r,s), (r',s')$ with $f(r,s) > 0 > f(r',s')$.

If $a > 0$ consider $-f$. If $a = 0$, $c \neq 0$ consider $f(1,y)$ instead. If $a = c = 0$ then $f = bxy$ and $b = \pm\sqrt{d} \neq 0$, so obviously indefinite.

(iv) $\alpha = \beta$, left as an exercise. □

Note. We can have $a, b, c > 0$ but f indefinite, for instance $(1,3,1)$ which has $d > 0$. We can also have $b < 0$ but f positive definite, for example $(1,-1,2)$ which has $d < 0$.

From now on, we restrict to positive definite BQFs (a,b,c) with $a, c > 0$ and $d = b^2 - 4ac < 0$. The first aim is to identify the 'simplest' or 'smallest' form in each equivalence class.

Example. Take $(10, 34, 29)$ and we look for equivalent forms with smaller coefficients (this has $d = -4$). First try to reduce $b = 34$ by replacing x with $x + \lambda y$ for suitable λ.

$$f(x,y) = ax^2 + bxy + cy^2 \implies f(x+\lambda y, y) = x^2 + (b + 2\lambda a)xy + (\lambda^2 a + \lambda b + c)y^2$$

Take $\lambda = \pm 1$, so

$$(a,b,c) \sim (a, b \pm 2a, a \pm b + c) \qquad (*)$$

and in our example $(10,34,29) \sim (10,14,5) \sim (10,-6,1)$.

To reduce the size of a, apply $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ so $X = y$, $Y = -x$ and

$$(a,b,c) \sim (c,-b,a) \qquad (**)$$

In the example,

$$(10,-6,1) \overset{(**)}{\sim} (1,6,10)$$
$$\overset{(*)}{\sim} (1,4,5)$$
$$\overset{(*)}{\sim} (1,2,2)$$
$$\overset{(*)}{\sim} (1,0,1)$$

Remark.

- Applying ($*$) repeatedly, we can replace f by an equivalent form with the same a and $|b| \le a$.
- Applying ($**$) repeatedly, we can replace f by an equivalent form with $a \le c$ and $|b|$ unchanged.

Definition (Reduced)**.** A positive definite BQF is **reduced** if either

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

Note that in both cases $|b| \le a \le c$.

In the example, $(10, 34, 29)$ is not reduced as $|b| \not\le a$, but $(1, 0, 1)$ is.

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

Proof. Consider the unimodular substitutions

$$T_\pm = \begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix} : (a, b, c) \longmapsto (a, b \pm 2a, a \pm b + c)$$
$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : (a, b, c) \longmapsto (c, -b, a)$$

If $a > c$, apply S to replace f with an equivalent form with smaller a but $|b|$ unchanged. If $a \le c$ and $|b| > a$, use one of $T_\pm$ to decrease $|b|$ (as $|b \pm 2a| < |b|$ for some $\pm$ since $a < |b|$) leaving a unchanged.

Repeat. At each step, $a + |b|$ is decreased, and $a + |b| > 0$. So the process must terminate; after a finite number of substitutions, we reach a form (a, b, c) with $|b| \le a \le c$. There are two cases:

a) $a < c$: then (a, b, c) will be reduced unless $b = -a$ and then

$$(a, b, c) = (a, -a, c) \sim (a, a, c)$$

which is reduced since $-a < b = a < c$.

b) $a = c$, then (a, b, c) will be reduced provided $0 \le b \le a$. Otherwise, $-a \le b < 0$ and then $(a, b, c) = (a, b, a) \sim (a, -b, a)$ which is reduced. □

Remark. We showed that our form was equivalent to a reduced form using only the substitutions S, $T_\pm$. With a bit more work, this shows that any unimodular substitution may be written as a product of Ss and $T_\pm$s, so $\mathrm{SL}_2(Z)$ is generated by S and $T_\pm$.

Lemma 4.6. Let $f = (a, b, c)$ be a reduced positive definite BQF, $d = b^2 - 4ac < 0$. Then

$$|b| \le a \le \sqrt{\frac{|d|}{3}} \quad \text{and} \quad b \equiv d \pmod 2.$$

Remark. For fixed d, there are only finitely many possible (a, b), and $c = \frac{b^2 - d}{4a}$, so there is only a finite number of reduced forms of discriminant d.

Proof. $b^2 \equiv d \pmod 4$ so $b \equiv d \pmod 2$. f is reduced $\implies |b| \le a \le c$, and

$$d = b^2 - 4ac \le ac - 4ac = -3ac \le -3a^2, \implies a^2 \le \frac{1}{3}|d|. \qquad \square$$

Example. Take $d = -4$. Then $|b| \le a \le 1$, and $b \equiv 0 \pmod 2$ so $a = 1, b = 0 \implies c = 1$. So the only reduced BQF of discriminant -4 (positive definite) is $x^2 + y^2$.

Use this to prove the 'serious' part of Theorem 4.1: if $p \equiv 1 \pmod 4$ then $p = x^2 + y^2$, $x, y \in \mathbb{Z}$.

Proof. $p \equiv 1 \pmod 4 \Rightarrow \left(\frac{-1}{p}\right) = 1$, so $\exists u, k \in \mathbb{Z}$ such that $u^2 = -1 + pk$. Let $f = (p, 2u, k)$. Then $f(1, 0) = p$, $\operatorname{disc}(f) = 4u^2 - 4pk = -4$.

But by Lemma 4.5 and the last calculation, f is equivalent to $x^2 + y^2$. So $\exists x, y \in \mathbb{Z}$ such that $x^2 + y^2 = p$. $\square$

This method can be applied more generally. Note if $f(x, y) = n$ then $f(kx, ky) = k^2 n$. Recall f represents n if $\exists x, y \in \mathbb{Z}$ such that $f(x, y) = 1$.

Definition (Proper representation)**.** f **properly represents** n if $\exists x, y \in \mathbb{Z}$ such that $f(x, y) = n$ and $(x, y) = 1$ (in particular $(x, y) \neq (0, 0)$.)

Remark. Suppose $f(x, y) = g(X, Y)$ with $\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ and $\alpha\delta - \beta\gamma = 1$, so $\begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$. For $x, y \in \mathbb{Z}$, $\gcd(x, y) = \gcd(X, Y)$, so f, g 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, and $a - |b| + c$ in that order.

A number in this list is repeated $\iff$ it is (properly) represented by f in more than one way – excluding $f(x, y) = f(-x, -y)$. For example, take $f = x^2 + y^2 = (1, 0, 1)$. $f(1, 0) = a = f(0, 1) = c < f(1, 1) = 2 = a - |b| + c$.

Proof. If $f(x, 0) = n$ properly, then $(x, y) = 1 \Rightarrow x = \pm 1 \Rightarrow n = f(1, 0) = a$. If $f(0, y) = n$ properly, then $y = \pm 1 \Rightarrow n = f(0, 1) = c$.

Suppose $n = f(x, y), |x| \ge |y| > 0$, $\gcd(x, y) = 1$. Then

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

For a choice of sign, $f(1, \pm 1) = a \pm b + c = a - |b| + c$. So $a \le c \le a - |b| + c$ are the least values properly represented by f. $\square$

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

Proof. By Lemma 4.5, every positive definite BQF is equivalent to some reduced form, so have to show that if $f \sim g$ and f, g are reduced, then $f = g$. Say $f = (a, b, c) \sim g = (a', b', c')$ are both reduced.

By Lemma 4.7, the least n properly represented by f is a, and by g is a', so $a = a'$. The next least integer properly represented by f is c, and by g is c', so $c = c'$. So, $b^2 = d + 4ac =$

$d + 4a'c' = b'^2$, so $g = (a, b, c)$ or $g = (a, -b, c)$. We need to take care of $a = c$: if $a = c$ then (a, b', a) is reduced $\iff 0 \le b' \le a$, so $(a, -b, a)$ is excluded and $f = g$.

Otherwise $a < c$, $-a < b \le a$. If $(a, -b, c)$ is reduced then $-a < b < a$. Then $a < c < a - |b| + c$ (no repeats). By the proof of Lemma 4.7

$$f(x, y) = \begin{cases} a & \iff (x, y) = (\pm 1, 0) \\ c & \iff (x, y) = (0, \pm 1) \end{cases}$$

and same for g. As $g(x, y) = f(X, Y)$, $\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ so

$$(x, y) = (\pm 1, 0) \iff f = a = g \iff (X, Y) = (\pm 1, 0).$$

Similarly, $(x, y) = (0, \pm 1) \iff (X, Y) = (0, \pm 1)$ so $\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$. As $\alpha\delta - \beta\gamma = 1$, $\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, hence $g(x, y) = f(\epsilon x, \epsilon y) = f(x, y)$. □

Remark. The definition of 'reduced' was cooked up precisely to ensure that this Theorem holds.

Example. For $d = -24$, $x^2 + 6y^2$ and $2x^2 + 3y^2$ are reduced and inequivalent, with disc $= -24$. Are there others? $|b| \le a \le \sqrt{8}$ so $|b| \le a \le 2$, and $b = d = 0 \pmod 2$.

For $a = 1$, we have $b = 0$ so $c = 6$, giving $(1, 0, 6)$.

For $a = 2$, $b \in \{0, \pm 2\}$ and $c = \frac{b^2+24}{8}$. $b = \pm 2 \implies c \notin \mathbb{Z}$, so $b = 0$ and $c = 3$ giving $(2, 0, 3)$. So there are no others.

Every positive definite BQF is equivalent to a unique reduced form, and $\exists$ only a finite number of reduced forms of discriminant d.

Definition (Class number)**.** The number of positive definite reduced forms of discriminant d is called the **class number** $h(d)$.

Example. $h(-4) = 1 = h(-7)$, and $h(-24) = 2$.

We saw that for given d, we can easily work out what the reduced forms are. How does $h(d)$ behave as a function of d? How many d are there with $h(d) = 1$? Some results (beyond the scope of this course), mostly using analytic number theory:

1. $h(d) \to \infty$ as $d \to -\infty$ (1934 Heilbronn), so $\#\{\, d \mid h(d) \le X \,\}$ is finite. First Siegel showed $h(d) \to \infty$ assuming the generalised Riemann hypothesis in analytic number theory. Then Heilbronn proved $h(d) \to \infty$ assuming GRH false by a completely different method.

2. 'On average $h(d) \approx \sqrt{|d|}$':

$$\frac{1}{\frac{1}{2}X} \sum_{\substack{0 \ge d \ge -x \\ d \equiv 0,1 \bmod 4}} h(d) \sim c\sqrt{X} \text{ for some } c > 0. \qquad \text{(1874, Mertens)}$$

3. $h(d) = 1 \iff -d = 3, 4, 7, 8, 11, 19, 43, 67, 163$ and $12, 16, 27, 28$. It was known since around 1900 that this was true, except for possibly one other d with $-d$ very large. (1967 Baker, Stark showed the list was complete, but was actually proved 10 years earlier by Heeger).

4. $\{\, d \mid h(d) \leq 100 \,\}$ is known. In fact $\exists$ explicit bound for the largest $|d|$ with $h(d) = N$, but it is not very practical, for $N = 1$ is is e^{5000}. This is nevertheless a very hard result using analytic number theory, algebraic geometry and elliptic curves.

Now study the problem: if f is a BQF and $n \in \mathbb{Z}$, when does f represent n? We've seen the answer for $x^2 + y^2$. Now partially generalise this to positive definite BQFs. For indefinite forms look at the section on continued fractions: the method is very different.

Lemma 4.9. Let f be a BQF, $n \in \mathbb{Z}$. Then f properly represents $n \iff f \sim g = (a, b, c)$ with $a = n$.

Proof. ($\Leftarrow$). $g(n, b, c) \Rightarrow g(1, 0) = n$, so g represents n properly. Hence if $f \sim g$, so does g.

($\Rightarrow$) f properly represents n means $\exists \gamma, \delta \in \mathbb{Z}$ with $f(\gamma, \delta) = n$ and $(\gamma, \delta) = 1$. Then $\exists \alpha, \beta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1$ by Euclid. Let $g(x, y) = f(\gamma x + \alpha y, \delta x + \beta y) \sim f$. Then $g(1, 0) = f(\gamma, \delta) = n$, i.e. $g = (n, b, c)$. □

Recall $p = x^2 + y^2 \iff p = 2$ or $\left(\frac{-1}{p}\right) = 1$. Generalise:

Theorem 4.10. Let $d < 0$ be a discriminant (i.e. $d \equiv 0$ or $1 \bmod 4$), and say $n \geq 1$. Then

$$\begin{aligned} &n \text{ is properly represented by some BQF of discriminant } d \\ \iff &x^2 \equiv d \pmod{4n} \text{ is soluble.} \end{aligned}$$

Proof. ($\Rightarrow$) Suppose $n = f(x, y)$ properly, and $\operatorname{disc}(f) = d$. Then Lemma 4.9 $\Rightarrow f \sim g = (n, b, c)$ with $b, c \in \mathbb{Z}$ and $d = \operatorname{disc}(g) = b^2 - 4cn \implies b^2 \equiv d \pmod{4n}$.

($\Leftarrow$) Suppose soluble. $\exists b, c \in \mathbb{Z}$ with $b^2 = d + 4nc$. Then (n, b, c) has discriminant d, and properly represents n. □

Example. What integers are represented (properly) by $f = x^2 + xy + 2y^2$? $\operatorname{disc}(f) = -7$. f is reduced. If (a, b, c) is any other reduced form of the same discriminant then $|b| \leq a \leq \sqrt{\frac{7}{3}}$ and $b \equiv d \pmod 2$ is odd, so $a = 1$, $b = \pm 1$, $c = 2$ and (a, b, c) reduced $\implies (a, b, c) = (1, 1, 2)$ so $h(-7) = 1$.

Let's first consider $f(x, y) = p$, p prime, $p \neq 2, 7$. By Theorem 4.10, p is properly represented by $f \iff x^2 \equiv -7 \pmod{4p}$ is soluble

$$\begin{aligned} &\iff \begin{cases} x^2 \equiv -7 \pmod 4 \\ x^2 \equiv -7 \pmod p \end{cases} \quad \text{are soluble} \\ &\iff \left(\frac{-7}{p}\right) = 1. \end{aligned}$$

But

$$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)(-1)^{\frac{p-1}{2}}\left(\frac{p}{7}\right) = \left(\frac{p}{7}\right) = \begin{cases} 1 & p \equiv 1, 2, 4 \pmod 7 \\ -1 & p \equiv 3, 5, 6 \pmod 7 \end{cases}.$$

Also $f(0, 1) = 2$ and $f(1, -2) = 7$.

So, a prime p is properly represented $\iff p = 7$ or $p \equiv 1, 2, 4 \pmod 7$.

For more general n, let $n = 2^{e_2}3^{e_3}\cdots = \prod_p p^{e_p}, e_p \geq 0$ and $e_p = 0$ for all but finitely many p. Then

$$x^2 \equiv d \pmod{4n} \text{ is soluble} \iff \left.\begin{array}{ll} \forall p \neq 2 & x^2 \equiv d \pmod{p^{e_p}} \\ \text{and} & x^2 \equiv d \pmod{2^{e_p+2}} \end{array}\right\} \text{ are soluble}$$

The next goal is to show if $x^2 \equiv d \pmod{p}$ soluble ($p \nmid d$), then the congruence is soluble mod p^e $\forall e \geq 1$ for p odd, i.e. that the Legendre symbol determines solubility.

Lemma 4.11.

(i) Take p an odd prime, $a \in \mathbb{Z}$ with $\left(\frac{a}{p}\right) = 1$. Then $\forall n \geq 1$, $x^2 \equiv a \pmod{p^n}$ is soluble.

(ii) $a \equiv 1 \pmod 8 \implies x^2 \equiv a \pmod{2^n}$ soluble $\forall n \geq 1$.

Proof.

(i) $\left(\frac{a}{p}\right) = 1 \implies$ there is a solution to $x^2 \equiv a \pmod p$. So, by induction assume that for some $n \geq 1$, $x^2 = a + kp^n$ for some $k \in \mathbb{Z}$. Consider $t \in \mathbb{Z}$, so

$$\begin{aligned}(x + tp^n)^2 &= x^2 + 2xtp^n + t^2p^{2n} \\ &\equiv a + (k + 2xt)p^n \pmod{p^{n+1}}.\end{aligned}$$

Since $\left(\frac{a}{p}\right) \neq 0$, $(a, p) = 1 = (x, p)$. So, $\exists t \in \mathbb{Z}$ such that $k + 2xt \equiv 0 \pmod p$. For this t, $(x + p^n t)^2 \equiv a \pmod{p^{n+1}}$.

(ii) $n \leq 3$ is easy, take $x = 1$. So again by induction, assume $x^2 = a + 2^n k$ for $n \geq 3$. If k even, then $x^2 \equiv a \pmod{2^{n+1}}$. Otherwise,

$$\begin{aligned}(x + 2^{n-1})^2 = x^2 + x2^n + 2^{2n-2} &\equiv a + (x + k)2^n \pmod{2^{n+1}} \\ &\equiv a \pmod{2^{n+1}}.\end{aligned}$$

□

Example. Continuing the example of $f = (1, 1, 2)$ with disc $= -7$:

- $-7 \equiv 1 \pmod 8 \implies x^2 \equiv -7 \pmod{2^n}$ is soluble $\forall n$.
- For p odd and $p \equiv 1, 2, 4 \pmod 7$, $\left(\frac{-7}{p}\right) = 1 \implies x^2 \equiv -7 \pmod{p^n}$ is soluble $\forall n \geq 1$.
- For $p = 7$: $x^2 \equiv -7 \pmod 7$ is soluble, but $x^2 \equiv -7 \pmod{49}$ is insoluble, hence insoluble mod 7^n $\forall n \geq 2$.

Conclusion: $f = (1, 1, 2)$ properly represents $n \geq 1$ if and only if

$$n = 2^{e_2}7^{e_7}\prod_{p \equiv 1,2,4 \bmod 7} p^{e_p}, \qquad e_p \geq 0,\ e_7 \in \{0, 1\}$$

The numbers represented (not necessarily properly) by f are k^2n, $k \geq 1$ with n as above. That is, $n = x^2 + xy + 2y^2$ for some $x, y \in \mathbb{Z}$ if and only if $n = 0$ or every prime $p \not\equiv 1, 2, 4 \pmod 7$ dividing n divides it to an even power.

This method completely describes the integers represented by f of discriminant $d < 0$ when $h(d) = 1$. For $h(d) > 1$, all this tells us is which n are represented by *some* equivalence class of BQFs of discriminant d.

Sometimes (as on the example sheet), you can figure out which just by congruence conditions, but usually not. For example, $x^2 + 23y^2$ - the representability of n by $x^2 + 23y^2$ cannot be described using congruence conditions on $p \mid n$. (Why? Deep algebraic number theory related to 'non-abelian reciprocity laws'.)

Definition (Fundamental discriminant)**.** $d \equiv 0$ or $1 \pmod 4$ is a **fundamental discriminant** if $d \neq k^2 d'$, where $k \geq 2$ and $d' \equiv 0$ or $1 \pmod 4$.

For fundamental discriminant $d < 0$, Gauss defined composition of two BQFs of discriminant d to get a third, turning {equivalence classes of positive definite BQFs of discriminant d} into an abelian group, the class group. This turns out to be the ideal class group of the quadratic field $\mathbb{Q}(\sqrt{d})$ (see Number Fields).

Negative definite forms now provide nothing new, but what about indefinite forms?

The key difference between definite and indefinite forms is that for a definite form f, $\#\{(x, y) \in \mathbb{Z}^2 \mid f(x, y) = n\}$ is always finite. For instance, $x^2 + y^2 = n \implies |x|, |y| \leq \sqrt{n}$. In general, $f(x, y) = n$ is the equation of an ellipse in $\mathbb{R}^2$, so integer points (x, y) on it have bounded size.

On the other hand, if f is indefinite, then there can be infinitely many solutions. For example, $x^2 - 2y^2$ is indefinite. Consider $x^2 - 2y^2 = 1$. We have solutions $(x, y) = (1, 0)$ and also $(3, 2)$. If (x, y) is a solution, then $(x^2 + 2y^2)^2 - 2(2xy)^2 = (x^2 - 2y^2)^2 = 1$ as well. So starting with $(3, 2)$ and repeating gets solutions of arbitrarily large size. We study $x^2 - dy^2 = 1$ later.

What about more variables? For instance, what integer values does $x_1^2 + x_2^2 + \cdots + x_k^2$ take?

Theorem (1770, Lagrange)**.** Every positive integer n is a sum of four squares. So for $k \geq 4$, we are done.

Proof. Not in the scope of this course, but there is a formula for the number of representations involving 'modular forms'. □

Harder is

Theorem (1797, Legendre)**.**

$$n = x^2 + y^2 + z^2 \iff n \neq 4^a(8b + 7)$$

Proof. The $\implies$ direction is easy, and the usual proof of $\impliedby$ is hard and uses quadratic reciprocity, and Dirichlet's theorem on existence of primes in arithmetic progressions. Again, this is out of scope. □

5 Distribution of the primes

We consider the sequence of primes,

$$2, 3, 5, 7, 11, 13, 17, \ldots, 691, \ldots, 144169, \ldots$$

an infinite sequence (Euclid).

Two natural questions are:

(i) How rapidly does the sequence grow?

(ii) How (ir)regular is the sequence e.g. how big are the gaps?

(i) is partially answered by the

Theorem (Prime Number Theorem)**.**

$$\pi(X) \coloneqq \#\{\text{primes } p \le X\} \sim \frac{X}{\log X} \text{ as } X \to \infty$$
$$\sim \int_2^X \frac{dt}{\log t} \quad \text{logarithmic integral}$$

The proof uses complex analysis. We'll eventually prove

Theorem (Tchebyshev's Theorem)**.** $\exists c_2 > c_1 > 0$ such that

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

For the moment, we'll prove some weaker results:

Lemma 5.1.

$$\pi(x) \ge \frac{\log x}{2 \log 2} \quad \forall \text{integers } x \ge 1$$

Proof. Let $\{p_1, \ldots, p_r\} = \{\text{primes} \le x\}$ (so $\pi(x) = r$). If $n \le x$, $n = K^2 p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $1 \le K \le \sqrt{x}$, $\alpha_i \in \{0, 1\}$ (so K is the largest square dividing n).

$$\text{there are } \left.\begin{array}{ll} \le \sqrt{x} & \text{possibilities for } k \\ \le 2^r & \text{possibilities for } \alpha_i \text{s} \end{array}\right\} \implies x = \#\{1 \le n \le x\} \le \sqrt{x} 2^r$$
$$2^r = 2^{\pi(x)} \ge \sqrt{x} \implies \pi(x) \ge \frac{\log x}{2 \log 2}. \qquad \square$$

Say p_n is the n^{th} prime. On average, by the prime number theorem, $p_{n+1} - p_n$ is around $\log X$. But the gap oscillates wildly.

Small gaps: An old conjecture ('twin prime problem') says $\exists \infty$ many n with $p_{n+1} = p_n + 2$. Quite recently: it has been proved there is a constant C such that for infinitely many n, $p_{n+1} \le p_n + C$. The best known such constant is $C = 246$, from the Polymath project.

Big gaps: By the PNT, at least $\log p_n$ infinitely often.

We will prove:

Theorem (Bertrand's postulate)**.** $p_{n+1} \le 2p_n$, there is always a prime between N and $2N$.

Analytic number theory in fact shows that for n sufficiently large, $p_{n+1} - p_n \leq p_n^{0.525}$. In the other direction, there are infinitely many n such that

$$p_{n+1} - p_n > c\frac{\log p_n \log\log p_n \log\log\log\log p_n}{\log\log\log p_n}$$

(and $(\log p_n)^2$ is conjectured).

Theorem 5.2.

(i) $\sum_{p \text{ prime}} \frac{1}{p}$ is divergent

(ii) $\prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right)^{-1}$ is divergent i.e. $\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} \to \infty$ as $x \to \infty$.

Proof. First prove (ii)

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \leq x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) \geq \sum_{n \leq x} \frac{1}{n}.$$

If $n = p_1^{e_1} \cdots p_k^{e_k}$, all $p_i \leq x$ then $\frac{1}{n} = \frac{1}{p_1^{e_1}} \cdots \frac{1}{p_k^{e_k}}$ occurs in the product and all terms > 0. So as $\sum \frac{1}{n} \to \infty$, the product $\to \infty$ as $x \to \infty$.

For (i) take logarithms of this

$$\begin{aligned}
\log \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} &= \sum_{p \leq x} -\log\left(1 - \frac{1}{p}\right) \\
&= \sum_{p \leq x} \left(\frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + \cdots\right) \\
&= \sum_{p \leq x} \frac{1}{p} + R_x \\
R_x = \sum_{p \leq x} \left(\frac{1}{2p^2} + \frac{1}{3p^3} + \cdots\right) &\leq \sum_{p \leq x} \left(\frac{1}{p^2} + \frac{1}{p^3} + \cdots\right) \\
&= \sum_{p \leq x} \frac{1}{p(p-1)} \\
&\leq \sum_{m \geq 2} \frac{1}{m(m-1)} = 1.
\end{aligned}$$

As $\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} \to \infty$, so does $\log\left(\prod_{p \leq x}(1 - \frac{1}{p})^{-1}\right)$ and so does $\sum_{p \leq x} \frac{1}{p}$. □

To take these ideas further, Riemann introduced the Riemann ζ-function for complex variables

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

(previously considered by Euler for real $s > 1$).

Proposition 5.3. The series converges absolutely iff $\mathrm{Re}(s) > 1$.

Proof. Let $s = \sigma + it$, $\sigma, t \in \mathbb{R}$. Then

$$\left|\frac{1}{n^s}\right| = \left|\frac{1}{e^{\log n(\sigma+it)}}\right| = \frac{1}{n^\sigma}.$$

So the series is absolutely convergent $\iff \sum_{n\geq 1} \frac{1}{n^\sigma}$ converges $\iff \sigma > 1$. □

By complex analysis and uniform convergence $\implies \zeta(s)$ is an analytic function of s for $\mathrm{Re}(s) > 1$. What has ζ got to do with primes?

Theorem 5.4.

(i) $\zeta(s) = \prod_{p \text{ prime}} (1 - \frac{1}{p^s})^{-1}$ - the 'Euler product' ($\mathrm{Re}(s) > 1$).

(ii) $\zeta(s) \neq 0$ if $\mathrm{Re}(s) > 1$.

Proof.

(i) The aim is to show

$$\prod_{p\leq x} \left(1 - \frac{1}{p^s}\right)^{-1} \to \zeta(s) \text{ as } x \to \infty.$$

So,

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

where $\eta_x = \{\, n \geq 1 \mid \text{at least one prime factor of } n \text{ is } > x \,\}$

because

$$\prod_{p\leq x} (1 + p^{-s} + p^{-2s} + \cdots) = \sum_{\substack{n \text{ product} \\ \text{of primes} \\ \leq x}} n^{-s}$$

by unique factorisation. So

$$\begin{aligned}\left|\zeta(s) - \prod_{p\leq x} \left(1 - \frac{1}{p^s}\right)^{-1}\right| &\leq \sum_{n\leq\eta_x} n^{-\sigma} \qquad (\sigma = \mathrm{Re}(s) > 1) \\ &\leq \sum_{n>x} n^{-\sigma} \to 0 \text{ as } x \to \infty \text{ as } \sigma > 1.\end{aligned}$$

(ii)

$$\begin{aligned}\prod_{p\leq x} \left(1 - \frac{1}{p^s}\right) \cdot \zeta(s) &= \prod_{p>x} \left(1 - \frac{1}{p^s}\right)^{-1} \text{ by part (i)} \\ &= 1 + \sum_{\substack{n \text{ s.t.} \\ \text{all } p|n \\ \text{satisfy } p>x}} n^{-s} \to 1 \text{ as } x \to \infty\end{aligned}$$

so

$$\left|\prod_{p\le x}\left(1-\frac{1}{p^s}\right)\zeta(s)\right| \ge 1-\sum_{n>x} n^{-\sigma} > 0 \text{ if } x \text{ is large enough}$$
$$\implies \zeta(s)\neq 0. \qquad \square$$

Theorem 5.5. $\zeta(s)-\frac{1}{s-1}$ extends to an analytic function on $\{\mathrm{Re}(s)>0\}$ by analytic continuation.

(As $s\to 1$, the series representing $\zeta(s)$ becomes divergent, and we would like to subtract off the divergence. $\int_1^\infty \frac{dx}{x^{s-1}} = \frac{1}{s-1}$.)

Proof. Suppose $\mathrm{Re}(s)>2$ for the moment.

$$\begin{aligned}\zeta(s) = \sum_{n\ge1}\frac{1}{n^s} &= \sum_{n\ge1}\left(\frac{n}{n^s}-\frac{n-1}{n^s}\right) = \sum_{n\ge1}\frac{n}{n^s}-\sum_{n\ge2}\frac{n-1}{n^s}\\ &= \sum_{n\ge1}\frac{n}{n^s} = \sum_{n\ge1}\frac{n}{(n+1)^s} = \sum_{n\ge1} n\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right)\\ &= \sum_{n\ge1} n\int_n^{n+1} s\frac{dx}{x^{s+1}}\end{aligned}$$

since

$$\begin{aligned}\int_a^b \frac{dx}{x^s} &= \left[-\frac{x^{1-s}}{s-1}\right]_a^b\\ &= \frac{1}{s-1}\left(\frac{1}{a^{s-1}}-\frac{1}{b^{s-1}}\right)\end{aligned}$$

If $n\le x<n+1$ then $n=\lfloor x\rfloor$.

$$\begin{aligned}&= s\sum_{n\ge1}\int_n^{n+1}\frac{\lfloor x\rfloor}{x^{s+1}}\,dx = s\int_1^\infty \frac{\lfloor x\rfloor}{x^{s+1}}\,dx = s\int_1^\infty \frac{x}{x^{s+1}}-\frac{x-\lfloor x\rfloor}{x^{s+1}}\,dx\\ &= \underbrace{\frac{s}{s-1}}_{=\frac{1}{s-1}+1} - s\int_1^\infty \frac{x-\lfloor x\rfloor}{x^{s+1}}\,dx\end{aligned}$$

So $\sigma(s)-\frac{1}{s-1} = 1-s\int_1^\infty \frac{x-\lfloor x\rfloor}{x^{s+1}}\,dx$. As $0\le x-\lfloor x\rfloor<1$, the integral converges for $\mathrm{Re}(s+1)>1$, i.e. $\mathrm{Re}(s)>0$ and by complex analysis represents an analytic function there. $\square$

Remark.

(i) In fact (using a more subtle integral) can show that $\zeta(s)-\frac{1}{s-1}$ is analytic $\forall s\in\mathbb{C}$ and $\zeta(s)$ satisfies an interesting identity

$$\begin{aligned}\xi(s) &\coloneqq \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)\\ &= \xi(1-s)\end{aligned}$$

where Γ is the function which interpolates factorial: $\Gamma(s)=\int_0^\infty e^{-y}y^{s-1}\,dy$.

(ii) A key ingredient in the prime number theorem is that $\zeta(s) \neq 0$ if $s = 1 + it$, $t \neq 0$, (can't get this from the infinite product).

We will say a little more about series of the form $\sum_{n\geq 1} a_n n^{-s}$ (Dirichlet series). A useful tool for manipulating these (and for other purposes) is the Möbius function.

Recall Lemma 2.4:

Lemma 2.4. Let f be a multiplicative function. Then so is g, defined by

$$g(n) = \sum_{d|n} f(d)$$

How can we recover f from g?

Example. Try an example:

$$\begin{aligned} g(6) &= f(1) + f(2) + f(3) + f(6) \\ g(3) &= f(1) + f(3) \\ g(2) &= f(1) + f(2) \\ g(1) &= f(1) \\ \implies f(6) &= g(6) - g(2) - g(3) + g(1) \end{aligned}$$

This obviously works in general!

Definition (Möbius function)**.** The **Möbius function** $\mu : \mathbb{N} \to \{0, \pm 1\}$ is given by

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \cdots p_k \text{ is a product of } k \text{ distinct primes} \\ 0 & \text{otherwise (divisible by a square} > 1) \end{cases}$$

Exercise. μ is a multiplicative function.

Apply Lemma 2.4 to μ, let $\nu(n) = \sum_{d|n} \mu(d)$. Then ν is a multiplicative function. Now

$$\begin{aligned} \nu(p^k) &= \mu(1) + \mu(p) + \cdots + \mu(p^k) \\ &= \begin{cases} \mu(1) = 1 & \text{if } k = 0 \\ \mu(1) + \mu(p) = 0 & \text{if } k = 1 \\ 0 & \text{if } k > 1. \end{cases} \end{aligned}$$

So by multiplicativity

$$\nu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n = 0. \end{cases}$$

Proposition 5.6 (Möbius inversion formula)**.** Let $f : \mathbb{N} \to \mathbb{C}$ be any function, and $g(n) = \sum_{d|n} f(d)$. Then

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

Proof.

$$\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{e|\frac{n}{d}} f(e)$$
$$= \sum_{e|n} f(e) \underbrace{\sum_{d|\frac{n}{e}} \mu(d)}_{\nu(\frac{n}{e})} = f(n). \qquad \square$$

Definition (Dirichlet series)**.** The series

$$\sum_{n\geq 1} \frac{a_n}{n^s}$$

for s a (complex) variable is called a **Dirichlet series**.

This is absolutely convergent if $|a_n| \leq An^k$ for some k and $\mathrm{Re}(s) > k+1$. We can take products of Dirichlet series

$$\sum_{m\geq 1} \frac{a_m}{m^s} \sum_{n\geq 1} \frac{b_n}{n^s} = \sum_{m,n\geq 1} \frac{a_m b_n}{(mn)^s} = \sum_{N\geq 1} \frac{c_N}{N^s}, \qquad N = mn$$
$$\text{where } c_N = \sum_{d|N} a_d b_{\frac{N}{d}}$$

Example.

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

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

A Dirichlet series related to primes:

Theorem 5.5a.

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n\geq 1} \Lambda(n) n^{-s} = \frac{\log 2}{2^s} + \frac{\log 3}{3^s} + \frac{\log 2}{4^s} + \frac{\log 5}{5^s} + \frac{\log 7}{7^s} + \cdots$$
$$\text{where } \Lambda(n) = \begin{cases} \log p & n = p^k,\ p \text{ prime} \\ 0 & \text{otherwise} \end{cases} \qquad \text{(von Mangoldt function)}$$

Proof. Assume $s > 1$ is real (for complex s, same follows by analytic continuation).

$$-\frac{\zeta'(s)}{\zeta(s)} = -\frac{d}{ds} \log \zeta(s) = -\frac{d}{ds} \sum_{p \text{ prime}} \log\left(\frac{1}{1-p^{-s}}\right) \qquad \text{(Theorem 5.4)}$$
$$= \sum_{p \text{ prime}} \frac{(\log p) p^{-s}}{1-p^{-s}}$$
$$= \sum_{p \text{ prime}} \log p (p^{-s} + p^{-2s} + \cdots)$$
$$= \sum_{n\geq 1} \Lambda(n) n^{-s}.$$

(Exchange of $\frac{d}{ds}$ and $\sum$ is justified by uniform convergence.) $\square$

Define $\Psi(x) = \sum_{n \le x} \Lambda(n)$. It is not hard to show that

$$\pi(x) \sim \frac{\Psi(x)}{\log x}$$

so the prime number theorem is equivalent to $\Psi(x) \sim x$. This is proved by integrating $\frac{x^{s+1}}{s(s+1)} \frac{\zeta'(s)}{\zeta(s)}$ over suitable contours (the non-vanishing of $\zeta(s)$ for $\operatorname{Re} s = 1$ enters here).

Theorem (Dirichlet's theorem)**.** Let $a, N \in \mathbb{Z}$, $N > 1$, $(a, N) = 1$. There are infinitely many primes $\equiv a \pmod N$ (we have seen this already for $N = 4$, $a = 1$ and $a = -1$) i.e. the arithmetic progression $\{a, a + N, a + 2N, \dots\}$ contains ∞ many primes.

In fact, the proportion of primes in such an arithmetic progression is $\frac{1}{\varphi(N)}$.

Sketch proof. The proof involves Dirichlet series. Take this series

$$F_{a,N}(s) = \sum_{p \equiv a \bmod N} \frac{1}{p^s}$$

and show it has infinitely many terms. It is enough to show that the series diverges for $s = 1$. To get a handle on $F_{a,N}(s)$, write it as a linear combination of Dirichlet series of the form $\sum_p \frac{\chi(p)}{p^s}$, where $\chi(p)$ is a multiplicative function. □

Definition (Dirichlet character)**.** A **Dirichlet character** mod N is a function $\chi : \mathbb{N} \to \mathbb{C}$ such that

(i) $\chi(1) = 1$, $\chi(n) = 0$ if $(N, n) > 1$.

(ii) $\chi(n + N) = \chi(n)$ periodic mod N.

(iii) $\chi(mn) = \chi(m)\chi(n)$ $\forall m, n$.

So χ is just a homomorphism $(\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ extended to all n by $\chi(n) = 0$ if $(n, N) > 1$. An example is given by the Legendre/Jacobi symbol.

Fact. The function

$$f(n) = \begin{cases} 1 & \text{if } n \equiv a \pmod N \\ 0 & \text{if } n \not\equiv a \pmod N \end{cases}$$

for $(a, N) = 1$ is a linear combination of Dirichlet characters mod N.

Example. For $N = 3$, $\chi_p : \mathbb{N} \to \mathbb{C}$:

$$\chi_0(n) = \begin{cases} 1 & \text{if } (n, 3) = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$\chi_1(n) = \begin{cases} 1 & n \equiv 1 \pmod 3 \\ -1 & n \equiv -1 \pmod 3 \\ 0 & (n, 3) \neq 1 \end{cases}$$

$$\frac{\chi_0(n) \pm \chi_1(n)}{2} = \begin{cases} 1 & n \equiv \pm 1 \pmod 3 \\ 0 & \text{otherwise} \end{cases}$$

Analytic facts about $L(\chi, s) = \sum_{n \ge 1} \chi(n) n^{-s}$ then can be used to prove Dirichlet's theorem.

5.1 Elementary methods for primes

Sieve of Eratosthenes: if you delete from $\{2, 3, \ldots, X\}$ all multiples of primes $\leq \sqrt{X}$, you are left with $\{\, p \text{ primes} \mid \sqrt{X} \leq p \leq X \,\}$.

Proposition 5.6a (Legendre's formula)**.** Let $x \geq 1$ and write $P = \prod_{p \leq \sqrt{X}} p$ product of all primes $\leq \sqrt{X}$. Then

$$\pi(X) - \pi(\sqrt{X}) + 1 = \#\{\, 1 \leq n \leq X \mid (n, P) = 1 \,\} = \sum_{d \mid P} \mu(d) \left\lfloor \frac{X}{d} \right\rfloor.$$

Proof.

$$\{\, 1 \leq n \leq X \mid (n, P) = 1 \,\} = \{1\} \cup \{\, p \mid \sqrt{X} \leq p \leq X \,\}$$

hence first equality. Recall

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

so

$$\begin{aligned} \#\{\, 1 \leq n \leq X \mid (n, P) = 1 \,\} &= \sum_{1 \leq n \leq X} \left[\sum_{d \mid (n, P)} \mu(d) \right] \\ &= \sum_{d \mid P} \mu(d) \sum_{\substack{1 \leq n \leq X \\ n \equiv 0 \bmod d}} 1 \\ &= \sum_{d \mid P} \mu(d) \left\lfloor \frac{X}{d} \right\rfloor. \end{aligned}$$

□

5.2 Divisibility of special numbers

Definition (Valuation)**.** Let $n \geq 1$, p prime. Let $\nu_p(n)$ = exponent of p in factorisation of n (p**-adic valuation** of n).

So $n = p^{\nu_p(n)} n_0$ where $(n_0, p) = 1$. In addition, $\nu_p(mn) = \nu_p(m) + \nu_p(n)$.

Example.

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

If $n < p \leq 2n$, p exactly divides numerator, and doesn't divide the denominator. So $\nu_p(n) = 1 \ \forall p \in (n, 2n]$.

On the other hand $N \leq \sum_r \binom{2n}{r} = 2^{2n}$, so $\prod_{n < p \leq 2n} p \leq N \leq 2^{2n}$, giving an estimate and upper bound for $\pi(x)$. A similar argument also gives a lower bound if more careful.

Lemma 5.7. Let $N = \binom{2n}{n}$, $n \geq 1$. Then

(i) $\frac{2^{2n}}{2n} \leq N \leq 2^{2n}$

(ii) For p prime, $n < p \leq 2n \implies \nu_p(N) = 1$

(iii) $\frac{2n}{3} < p \leq n \implies (N, p) = 1$

(iv) $p^k \mid N \implies p^k \leq 2n$ for any prime power p^k.

Proof.

(i)
$$N < \sum_{m=0}^{2n} \binom{2n}{m} = (1+1)^{2n} = 2^{2n} = 2 + \sum_{1 \leq m \leq 2n-1} \binom{2n}{m} \leq 2 + (2n-1)N \leq 2nN$$

(ii) $n < p \leq 2n < 2p \implies p$ divides numerator $2n \cdots (n+1)$ exactly but not denominator $n(n-1) \cdots 1$ of N.

(iii) $p \in (\frac{2}{3}n, n] \Rightarrow p \leq n < 2p \leq 2n < 3p \Rightarrow p$ divides both numerator and denominator exactly $\Rightarrow (p, N) = 1$.

(iv) For the last part we need the following formula, proved on Example Sheet 3
$$\nu_p(n!) = \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots$$

Lemma. If $x \geq 0$ then $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0, 1\}$.

Proof. $x = n + \alpha$ with $0 \leq \alpha < 1$. Then, LHS $= \lfloor 2\alpha \rfloor - 2\lfloor \alpha \rfloor = \begin{cases} 0 & 0 \leq \alpha < \frac{1}{2} \\ 1 & \frac{1}{2} \leq \alpha < 1 \end{cases}$. □

So,
$$\begin{aligned} \nu_p(N) &= \nu_p((2n)!) - 2\nu_p(n!) \\ &= \sum_{i \geq 1} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right) \end{aligned}$$
and if $p^k > 2n$
$$= \sum_{1 \leq i \leq k-1} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right) \leq k - 1 \quad \text{so } \nu_p(N) = k \Rightarrow p^k \leq 2n. \qquad \square$$

Use this to prove:

Theorem 5.8 (Tchebyshev's theorem)**.** $\exists c_2 > c_1 > 0$ such that $\forall x \geq 3$,
$$c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x}$$

We will show $c_1 = \frac{\log 2}{2} = 0.346...$ and $c_2 = 6 \log 2 = 4.158...$.

Proof. **Upper bound:** First claim $\pi(2^k) \leq 3\frac{2^k}{k}$. True for $k \leq 6$ as $\pi(x) \leq \frac{x}{2}$ if x even ≥ 4. By Lemma 5.7 (i) and (ii),
$$n^{\pi(2n) - \pi(n)} \leq \prod_{n < p \leq 2n} p \overset{\text{(ii)}}{\leq} N \overset{\text{(i)}}{\leq} 2^{2n}$$
$$\implies \pi(2n) - \pi(n) \leq 2 \log 2 \cdot \frac{n}{\log n}$$

$$\implies \pi(2^{k+1}) \le \pi(2^k) + \frac{2^{k+1}}{k} \le 3\frac{2^k}{k} + \frac{2^{k+1}}{k} \qquad \text{(induction on } k\text{)}$$
$$= \frac{5 \cdot 2^{k+1}}{2k} \le \frac{3}{k+1} 2^{k+1} \qquad (k \ge 5)$$

proving the claim.

Observe $\frac{x}{\log x}$ is monotonically increasing for $x \ge e$ (check by differentiating). So if

$$4 \le 2^k < x < 2^{k+1} \implies \pi(x) \le \pi(2^{k+1}) \le 6 \cdot \frac{2^k}{k+1} < 6 \cdot \frac{2^k}{k}$$
$$= 6 \log 2 \cdot \frac{2^k}{\log 2^k} \le 6 \log 2 \cdot \frac{x}{\log x}.$$

Lower bound: Lemma 5.7(iv) $\implies \forall p, p^{\nu_p(N)} \le 2n$ i.e. $\nu_p(N) \le \frac{\log 2n}{\log p}$ (and $= 0$ if $p > 2n$). Now $\frac{2^{2n}}{2n} \le N$ so

$$n \log 2 - \log 2n \le \log N = \sum_{p \le 2n} \nu_p(N) \log p \qquad \text{(as } N = \textstyle\prod p^{\nu_p(N)}\text{)}$$
$$\le \sum_{p \le 2n} \log(2n) = \pi(2n) \log(2n)$$
$$\implies \pi(2n) \ge \frac{2n \log 2}{\log 2n} - 1$$

So if $2n \le x < 2n + 2$

$$\pi(x) \ge \pi(2n) \ge \log 2 \cdot \frac{2n}{\log 2n} - 1 \ge \log 2 \cdot \frac{x-2}{\log x} - 1$$
$$= \log 2 \cdot \frac{x}{\log x} - \left(\frac{2 \log 2}{\log x} + 1 \right)$$
$$\ge \frac{1}{2} \log 2 \frac{x}{\log x} \quad \text{if } x \ge 16.$$

If $3 \le x \le 16$, $\frac{1}{2} \log 2 \cdot \frac{x}{\log x} < \frac{16}{2 \cdot 4} = 2 \le \pi(x)$. □

Tchebyshev actually showed

$$0.92 < \frac{\pi(x)}{x/\log x} < 1.11 \text{ for } x \text{ sufficiently large.}$$

Theorem 5.9 (Bertrand's postulate)**.** $\forall n > 1 \; \exists$ prime p with $n < p < 2n$.

First proved by Tchebyshev, this proof by Erdős.

Proof. Claim: Let $\Theta(x) \coloneqq \prod_{p \le x} p$. Then $\Theta(x) \le 4^x \quad \forall x \ge 1$ (proof deferred).

Suppose $\nexists p \in (n, 2n)$. Then by Lemma 5.7, if $p \mid N = \binom{2n}{n}$, $p \le \frac{2n}{3}$. Write $N = N_1 N_2$, where

$$N_1 = \prod_{\nu_p(N)=1} p \le \Theta\left(\frac{2n}{3}\right) \le 4^{2n/3}$$
$$N_2 = \prod_{\nu_p(N) \ge 2} p^{\nu_p(N)} \le (2n)^{\sqrt{2n}}$$

since $p^2 \le p^{\nu_p(N)} \le 2n$ by Lemma 5.7(iv), so $p \le \sqrt{2n}$. Therefore

$$\frac{2^{2n}}{2n} \le N = N_1 N_2 \le 4^{2n/3} \cdot (2n)^{\sqrt{2n}}$$

i.e. $2^{2n/3} \le (2n)^{1+\sqrt{2n}}$ or $\frac{\log 2}{3} \cdot 2n \le (1+\sqrt{2n}) \log 2n$.

This is false for $n \ge 500$, giving the required contradiction:

$$\frac{d}{dx}\left(\frac{\log 2}{3}x - (1+\sqrt{x})\log x\right) = \frac{\log 2}{3} - \frac{1+\sqrt{x}}{x} - \frac{\log x}{2\sqrt{x}} > 0 \text{ if } x \ge 300$$

For small n, $2, 3, 5, 7, 11, 19, 37, 73, 137, 277, 547$ fills the gap. □

Proposition. Let $\Theta(x) = \prod_{p \le x} p$. Then $\Theta(x) \le 4^x \quad \forall x \ge 1$.

Proof. Note that $2\binom{2n+1}{n} = \binom{2n+1}{n} + \binom{2n+1}{n+1} \le (1+1)^{2n+1} = 2^{2n+1}$.

Also if $n+2 < p \le 2n+1$ then $p \mid \binom{2n+1}{n+1}$ so

$$\prod_{n+2 \le p \le 2n+1} p \;\Bigg|\; \binom{2n+1}{n+1} \le 4^n$$

So if $n \ge 1$,

$$\begin{aligned}\Theta(2n+2) = \Theta(2n+1) = \prod_{p \le n+1} p \prod_{n+2 \le p \le 2n+1} p &\le \Theta(n+1) \cdot 4^n \\ &\le 4^{n+1} \cdot 4^n \text{ (induction on } n) \\ &= 4^{2n+1}.\end{aligned}$$

So, for all integers $n \ge 1$, $\Theta(n) \le 4^n$ and $\Theta(x) = \Theta(\lfloor x \rfloor)$. □

6 Continued Fractions

Consider the following problem: $\theta \in \mathbb{R}$, what are the 'best' rational approximations to Θ?

$$\left|\pi - \frac{314159}{100000}\right| < 3 \times 10^{-6}$$
$$\left|\pi - \frac{355}{113}\right| < 3 \times 10^{-7}$$

We would like a systematic way to get such approximations (where the error is small compared with the denominator).

6.1 Continued Fraction algorithm

Let $\theta \in \mathbb{R}$. Define a (possible finite) sequence of integers $a_0, a_1, \ldots$, with $a_n \geq 1$ for $n \geq 1$ as follows.

Step 0 $a_0 = \lfloor \theta \rfloor$. If $a_0 = \theta$, stop. Otherwise $0 < \theta - a_0 < 1$.
Let $\theta_1 = \frac{1}{\theta - a_0} > 1$ so that $\theta = a_0 + \frac{1}{\theta_1}$.

Step 1 $a_1 = \lfloor \theta_1 \rfloor$. If $a_1 = \theta_1$, stop.
Otherwise, let $\theta_2 = \frac{1}{\theta_1 - a_1} > 1$, so $\theta = a_0 + \frac{1}{a_1 + \frac{1}{\theta_2}}$.

Continue. If process stops at nth stage, i.e. $a_n = \theta_n$, then

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \\ a_{n-1} + \cfrac{1}{a_n}}}}$$

If it doesn't stop, for every n, $\theta = [a_0, \ldots, a_{n-1}, \theta_n]$ in this notation. We'll write $\theta = [a_0, a_1, \ldots]$ called the continued fraction expansion (CF) of θ (shortly we'll make sense of the $=$ sign here).

The integers $a_0, a_1, \ldots$ are the **partial quotients**.

Example. Take $\theta = \frac{59}{13}$.

$$\frac{59}{13} = 4 + \frac{7}{13} \qquad a_0 = 4, \theta_1 = \frac{13}{7}$$
$$\frac{13}{7} = 1 + \frac{6}{7} \qquad a_1 = 1, \theta_2 = \frac{7}{6}$$
$$\frac{7}{6} = 1 + \frac{1}{6} \qquad a_2 = 1, \theta_3 = 6$$

$a_3 = 6 = \theta_3$, so

$$\frac{59}{13} = [4, 1, 1, 6] = 4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6}}}$$

Clearly if the continued fraction algorithm for θ terminates, $\theta \in \mathbb{Q}$. Converse:

Proposition 6.1. The continued fraction expansion of θ terminates $\iff$ $\theta \in \mathbb{Q}$.

Proof. Let $\theta = \frac{b_0}{c_0}$, $\theta_i = \frac{b_i}{c_i}$, $b_i, c_i \in \mathbb{Z}$, $(b_i, c_i) = 1$ $c_i \geq 1$. If the continued fraction doesn't terminate, as $\theta_i \geq 1$, we must have $\theta_i > 1$ i.e. $b_i > c_i$.

$$\forall i \geq 1 \quad \theta_i = a_i + \frac{1}{\theta_{i+1}} \implies \frac{b_i}{c_i} = a_i + \frac{c_{i+1}}{b_{i+1}} \overset{(*)}{\implies} b_{i+1} = c_i < b_i$$

But b_i is then a decreasing sequence of positive $i > 0$ integers, so terminates. □

Remark. $(*)$ can be rewritten $b_i = a_i b_{i+1} + b_{i+2}$. So the sequence (b_i) comes from applying Euclid's algorithm to $(b_0, b_1 = c_0)$. For example, $\frac{59}{13} = \theta = \frac{b_0}{c_1}$,

$$\begin{aligned} 59 &= 4 \cdot 13 + 7 \\ 13 &= 1 \cdot 7 + 6 \\ 7 &= 1 \cdot 6 + 1 \\ 6 &= 6 \cdot 1 + 0 \end{aligned}$$

hence the terminology 'partial quotient'.

Definition (Convergents)**.** Given $a_0, a_1, \ldots, \in \mathbb{Z}$ $a_i \geq 1$ if $i \geq 1$ define sequence of integers p_n, q_n $(n \geq 0)$ recursively as follows

$$\begin{array}{lll} p_0 = a_0 & p_1 = a_1 a_0 + 1 & p_n = a_n p_{n-1} + p_{n-2} \\ q_0 = 1 & q_1 = a_1 & q_n = a_n q_{n-1} + q_{n-2} \quad \text{if } n \geq 2. \end{array}$$

It is convenient also to define $p_{-1} = 0$, $q_{-1} = 0$ (so the recursion holds for $n \geq 1$). If $[a_0, a_1, \ldots]$ is the CF expansion of θ, say $\frac{p_n}{q_n}$ are the **convergents** to θ.

As $a_i \geq 1$ if $i > 0$, $1 \leq q_1 < q_2 < q_3 < \cdots$ is an increasing sequence of positive integers.

Lemma 6.2.

(i) $\forall n \geq 0 \quad \frac{p_n}{q_n} = [a_0, \ldots, a_n]$.

(ii) Let $\beta > 0$ be real.

$$\frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}} = [a_0, a_1, \ldots, a_n, \beta]$$

and this number lies strictly between $\frac{p_n}{q_n}$ and $\frac{p_{n-1}}{q_{n-1}}$.

Proof.

(i) If we put $\beta = a_{n+1}$ in (ii) we get LHS $= \frac{p_{n+1}}{q_{n+1}}$ by the recursion formula, giving the required formula (replacing n with $n+1$).

(ii) Induct on n. For $n = 0$, $[a_0, \beta] = a_0 + \frac{1}{\beta} = \frac{\beta a_0 + 1}{\beta \cdot 1 + 0}$.

Let $\gamma = a_n + \frac{1}{\beta}$.

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

For the last part, if $\frac{x}{y} < \frac{x'}{y'}$ for $x, x', y, y' \in \mathbb{R}$ and $y, y' > 0$ then

$$\frac{x}{y} < \frac{x + x'}{y + y'} < \frac{x'}{y'}$$

(easy exercise), giving the required result. □

If $\theta = [a_0, \ldots, a_n]$ is rational, then Lemma 6.2 $\implies \theta = \frac{p_n}{q_n}$.

Lemma 6.3.

(i) $\forall n \geq 1$ (in fact, $n \geq 0$) $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$

(ii) $\forall n \geq 2$ (in fact, $n \geq 1$) $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$

Proof.

(i) Induction on n: $n = 0$ or 1 true. Assume true for $n - 1$. Then

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

by induction.

(ii) LHS:

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

by (i). □

Remark. As a consequence, (i) $\Rightarrow (p_n, q_n) = 1$ i.e. $\frac{p_n}{q_n}$ is in lowest terms and

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

From (ii),

$$\begin{aligned}\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} &= (-1)^n \frac{a_n}{q_n q_{n+2}} \\ \Rightarrow \frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}&\end{aligned}$$

and as $\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} \to 0$, $\frac{p_n}{q_n}$ converges.

If $[a_0, a_1, \ldots]$ is the CF expansion of θ by Lemma 6.2(ii), $\theta = [a_0, \ldots, a_n, \theta_{n+1}]$ lies between $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$ $\forall n$. This proves

Theorem 6.4. $\frac{p_n}{q_n} \to \theta$ as $n \to \infty$, and $\forall n \geq 0$

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

Remark. This actually shows that the CF expansion is a bijection

$$\{\theta \in \mathbb{R} \setminus \mathbb{Q}\} \longleftrightarrow \{\text{sequences } a_0, a_1, \ldots, \text{ where } a_n \in \mathbb{Z},\ a_n \geq 1 \text{ for } n > 0\}$$

6.2 Rational Approximations

Theorem 6.5. Let $\theta \in \mathbb{R} \setminus \mathbb{Q}$, $p, q \in \mathbb{Z}$, $0 < q < q_{n+1}$. Then

$$|q\theta - p| \geq |q_n\theta - p_n|$$

Corollary. If $p, q \in \mathbb{Z}$ and $\left|\theta - \frac{p}{q}\right| < \left|\theta - \frac{p_n}{q_n}\right|$ then $q > q_n$, so $\frac{p_n}{q_n}$ is the best approximation with denominator $\leq q_n$.

Proof of corollary. If $q \leq q_n < q_{n+1}$, by Theorem 6.5 $\left|\theta - \frac{p}{q}\right| \geq \frac{q}{q_n}\left|\theta - \frac{p_n}{q_n}\right| \geq \left|\theta - \frac{p_n}{q_n}\right|$. □

Proof of theorem. As $p_{n+1}q_n - p_n q_{n+1} = \pm 1$ $\exists u, v \in \mathbb{Z}$

$$\begin{pmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{pmatrix}\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} p \\ q \end{pmatrix} \quad \text{i.e.} \quad \begin{aligned} up_n + vp_{n+1} &= p \\ uq_n + vq_{n+1} &= q \end{aligned}$$
$$\therefore q\theta - p = u(q_n\theta - p_n) + v(q_{n+1}\theta - p_{n+1})$$

If $v = 0$, then $u \geq 1$ so $|q\theta - p| \geq u\,|q_n\theta - p_n| \geq |q_n\theta - p_n|$. So suppose $v \neq 0$, $0 < q < q_{n+1} \implies u \neq 0$ and u, v have opposite signs.

Now $q_n\theta - p_n$, $q_{n+1}\theta - p_{n+1}$ have opposite signs (θ lies between any two consecutive convergents). So $u(q_n\theta - p_n)$ and $v(q_{n+1}\theta - p_{n+1})$ have the same sign. Hence

$$|q\theta - p| = |u(q_n\theta - p_n) + v(q_{n+1}\theta - p_{n+1})| \geq |q_n\theta - p_n| \text{ as } u \neq 0.$$ □

Theorem 6.6. Let $\theta \in \mathbb{R} \setminus \mathbb{Q}$. Then

(i) at least one of any pair of successive convergents satisfies $\left|\theta - \frac{p}{q}\right| < \frac{1}{2q^2}$.

(ii) conversely if $\frac{p}{q} \in \mathbb{Q}$ satisfies (i) then $\frac{p}{q} = \frac{p_n}{q_n}$ for some n.

Proof.

(i) θ lies between $\frac{p_n}{q_n}$, $\frac{p_{n+1}}{q_{n+1}}$,

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

(the inequality follows from AM-GM) so either $\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2}$ or $\left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| < \frac{1}{2q_{n+1}^2}$

(ii) Suppose $q \geq 1$, $\left|\theta - \frac{p}{q}\right| < \frac{1}{2q^2}$. $\exists n$ such that $q_n \leq q < q_{n+1}$. Show $\frac{p}{q} = \frac{p_n}{q_n}$:

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

As $q < q_{n+1}$, Theorem 6.5 $\Rightarrow |q\theta - p| \geq |q_n\theta - p_n|$

$$< \left(\frac{1}{q} + \frac{1}{q_n}\right)\frac{1}{2q}$$

by the hypothesis on $\frac{p}{q}$.

If $\frac{p}{q} \neq \frac{p_n}{q_n}$, LHS$\geq \frac{1}{qq_n}$ so

$$\left(\frac{1}{q} + \frac{1}{q_n}\right)\frac{1}{2q} > \frac{1}{qq_n} \implies q < q_n,$$

a contradiction. □

Simplest irrationals

The simplest irrationals are the quadratic surds $\sqrt{d}$, for $d > 1$ not a square. Their CF expansions are computable and have nice properties.

Example.

$$\begin{aligned}
\theta &= \sqrt{6} = 2 + (\sqrt{6} - 2) && a_0 = 2\\
\theta_1 &= \frac{1}{\sqrt{6} - 2} = \frac{\sqrt{6} + 2}{2} = 2 + \frac{\sqrt{6} - 2}{2} && a_1 = 2\\
\theta_2 &= \frac{2}{\sqrt{6} - 2} = \sqrt{6} + 2 = 4 + (\sqrt{6} - 2) && a_2 = 4\\
\theta_3 &= \frac{1}{\sqrt{6} - 2} = \theta_1 \implies a_3 = 2 = a_1 = a_5 = a_7 = \cdots\\
&\implies \theta_4 = \theta_2 \text{ so } a_4 = 4 = a_2 = a_6 = \cdots
\end{aligned}$$

so $\theta = [2, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, \dots] = [2, \overline{2, 4}]$.

Definition (Eventually periodic)**.** The CF $[a_0, a_1, \dots, a_{m-1}, \overline{a_m, \dots, a_{m-k+1}}]$ is **eventually periodic**. The least k for which this holds is the period of the continued fraction. It is **purely periodic** if $m = 0$, i.e. $\theta = [\overline{a_0, \dots, a_{k-1}}]$.

Definition (Quadratic irrational)**.** θ is called a **quadratic irrational** if $\theta = r + s\sqrt{d}$, $r, s \in \mathbb{Q}$, $s \neq 0$, $d > 1$, non-square integer. Equivalently, $a\theta^2 + b\theta + c = 0$ for $a, b, c \in \mathbb{Z}$.

Theorem 6.7 (Lagrange)**.** The CF expansion of $\theta \in \mathbb{R} \setminus \mathbb{Q}$ is eventually periodic $\iff$ θ is a quadratic irrational.

Proof. ($\Rightarrow$). If $\phi = [\overline{a_0, \dots, a_{n-1}}]$ is purely periodic, then

$$\phi = [a_0, \dots, a_{n-1}, \phi] = \frac{p_{n-1}\phi + p_{n-2}}{q_{n-1}\phi + q_{n-2}} \implies \phi \text{ satisfies a quadratic equation.}$$

If $\theta = [a_1, \ldots, a_{n-1}, \overline{a_n, \ldots, a_{n+d-1}}]$ is eventually periodic,

$$\theta = \frac{p_{n-1}\theta_n + p_{n-2}}{q_{n-1}\theta_n + q_{n-2}} \text{ where } \theta_n = [\overline{a_n, \ldots, a_{n+d-1}}] = r + s\sqrt{D}$$

by the argument above. So,

$$\theta = \frac{p_{n-1}r + p_{n-2} + p_{n-1}s\sqrt{D}}{q_{n-1}r + q_{n-2} + q_{n-1}\sqrt{D}} = \frac{A + B\sqrt{D}}{A' + B'\sqrt{D}}$$
$$= \frac{(A + B\sqrt{D})(A' - B'\sqrt{D})}{A'^2 - B'^2 D}.$$

($\Leftarrow$) Suppose $a\theta^2 + b\theta + c = 0$ for $a, b, c \in \mathbb{Z}$, $a > 0$. Let $f(x, y) = ax^2 + bxy + cy^2$ (The BQF is indefinite as θ real).

$$\theta = \frac{p_n\theta_{n+1} + p_{n+1}}{q_n\theta_{n+1} + q_{n+1}} \implies f_n(\theta_{n+1}, 1) = 0 \text{ where}$$
$$f_n(x, y) = f(p_n x + p_{n+1}y, q_n x + q_{n+1}y) = A_n x^2 + B_n xy + C_n y^2$$

with

$$A_n = f_n(1, 0) = f(p_n, q_n) = f_{n+1}(0, 1) = C_{n+1}$$
$$\text{and } \operatorname{disc}(f_n) = \operatorname{disc}(f) \text{ as } \begin{vmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{vmatrix} = \pm 1$$

Claim: $\exists$ constant K such that $|A_n| \leq K$ $\forall n$. Suppose so: then $|C_n| = |A_{n-1}| \leq K$ and $B_n^2 - 4A_nC_n = \operatorname{disc}(f)$. As $A_n, B_n, C_n \in \mathbb{Z}$, there are only finitely many possibilities for f_n. Hence, for some $n, k > 0$, $\theta_{n+k} = \theta_n$.

Proof of claim: Let θ' be the other root of $a\theta^2 + b\theta + c = 0$. Then

$$\left| f\left(\frac{p_n}{q_n}, 1\right) \right| = a \underbrace{\left| \frac{p_n}{q_n} - \theta \right|}_{\leq \frac{1}{q_n^2}} \cdot \underbrace{\left| \frac{p_n}{q_n} - \theta' \right|}_{\to \theta - \theta'} \text{ since } f(x, 1) = (x - \theta)(x - \theta')$$

So $\left| f(\frac{p_n}{q_n}, 1) \right| \leq \frac{K}{q_n^2}$ $\forall n$, for some K, so $|A_n| = |f(p_n, q_n)| \leq K$. □

Remark. This doesn't tell us what the period of the continued fraction is. $\sqrt{6} = [2, \overline{2, 4}]$. $\sqrt{889} = [29, \overline{1, 4, 2, 3, \ldots, 1, 58}]$, length 42.

Theorem 6.8 (Galois)**.** Let θ be a quadratic irrational. Then the continued fraction for θ is purely periodic, iff $\theta > 1$ and $-1 < \theta' < 1$ where θ' is the other root of the quadratic. If so, then $-\frac{1}{\theta'} = [\overline{a_{n-1}, \ldots, a_0}]$.

Proof. Omitted in this course. □

Remark. Let $\theta = \sqrt{d}$, for $d > 1$ not a square. Then $\theta_1 = \frac{1}{\sqrt{d} - a_0} > 1$ and $\theta_1' = \frac{1}{-\sqrt{d} - a_0} \in (-1, 0)$. Hence θ_1 has a purely periodic CF, and $\sqrt{d} = [a_0, \overline{a_1, \ldots, a_n}]$.

Theorem 6.9. Let d be a positive integer, not a square. Then Pell's equation

$$x^2 - dy^2 = 1 \tag{$*$}$$

has a solution in integers $x, y \neq 0$ (in fact has infinitely many).

Proof.

$$\theta = \sqrt{d} = [a_0, \overline{a_1, \ldots, a_n}] = [a_0, a_1, \ldots, a_n, \theta_{n+1}]$$
$$\text{with } \theta_{n+1} = \theta_1 = [\overline{a_1, \ldots, a_n}] = \frac{1}{\sqrt{d} - a_0}$$
$$\implies \sqrt{d} = \frac{\theta_1 p_n + p_{n-1}}{\theta_1 q_n + q_{n-1}} = \frac{p_n + p_{n-1}(\sqrt{d} - a_0)}{q_n + q_{n-1}(\sqrt{d} - a_0)}$$

Multiply and equate coefficients of $1, \sqrt{d}$:

$$p_{n-1} = q_n - q_{n-1}a_0$$
$$d \cdot q_{n-1} = p_n - p_{n-1}a_0$$
$$\implies p_{n-1}^2 - dq_{n-1}^2 = p_{n-1}q_n - p_n q_{n-1} = (-1)^n$$

So if n is even, $(x, y) = (p_{n-1}, q_{n-1})$ is a solution of $(*)$. Otherwise, use $[a_0, \overline{a_1, \ldots, a_{2n}}]$ to get that $p_{2n-1}, q_{2n-1})$ is a solution. More generally, (p_{kn-1}, q_{kn-1}) is a solution $\forall k$ such that kn is even, so there are infinitely many solutions. □

Remark. We can also show (using the fact that $\frac{p_n}{q_n}$ are better approximations to θ than other rationals) that any solution (x, y) when $x, y > 0$ is (p_n, q_n) for some n.

Remark. If $x_1^2 - dy_1^2 = 1 = x_2^2 - dy_2^2$ then $X^2 - dY^2 = 1$ where

$$X + Y\sqrt{d} = (x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d})$$

This shows that the solutions of $(*)$ form a group under this operation. (See Number Fields 'units in quadratic fields'.)

7 Primality testing and factorisation

RSA relies on two properties:

1. if $N = pq$, where p, q are primes around 2^{500}, knowing N alone it is very hard to recover p, q.
2. there are easy to find large primes

To find a large prime, test numbers in a range for primality. By the prime number theorem, testing numbers of size M gives success after about $\log M$ tries. It would be useful to find some easy to check property which only holds for primes.

Recall Fermat's Little Theorem:

Theorem (Fermat's Little Theorem)**.** If p is prime and $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Example.

For $N = 15$, $2^{14} = (2^4)^3 \cdot 2^2 = 16^3 \cdot 4 \equiv 4 \pmod{15} \not\equiv 1 \pmod{15}$. So, 15 is not prime.

For $N = 91$, $3^{90} \equiv 1 \pmod{91}$, which gives no information. $2^{90} \equiv 64 \pmod{91}$, so 91 is not prime.

So we often have to use more than one value of a to get a good test. How many different a do we need to check $a^{N-1} \equiv 1 \pmod{N}$ to be sure N is prime? Or, if N is composite, how many a's do we need to try to detect this?

Definition (Pseudoprime)**.** Take N an odd, composite integer mod $b \geq 1$, $(b, N) = 1$. Say N is a (Fermat) **pseudoprime** to the base b if $b^{N-1} \equiv 1 \pmod{N}$. (This depends only on $b \bmod N$, so generally restrict to $1 \leq b < N$.)

Example. 91 is a Fermat pseudoprime base 3.

Notice if N is a pseudoprime to base b_1 and to base b_2, as $(b_1 b_2)^{N-1} = b_1^{N-1} b_2^{N-1}$, it is a pseudoprime to base $b_1 b_2$. Obviously every composite N is a pseudoprime to base 1. So $\{1 \leq b < N, (b, N) = 1 \text{ s.t. } N \text{ is a pseudoprime to base } b\}$ is a subgroup of the group $(\mathbb{Z}/n\mathbb{Z})^*$ of residue classes coprime to N under multiplication.

Proposition 7.1. Take $N > 1$, odd composite. If N is not a pseudoprime to some base, then for at least $\frac{1}{2}$ of $\{\, 1 \leq b < N \mid (b, N) \,\}$ it is not a pseudoprime to base b.

Proof.

$$H = \{\, b \mid N \text{ is a pseudoprime to base } b \,\}$$

is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. By hypothesis, it is a proper subgroup (as $\exists b \notin H$). By Lagrange, the order of H divides $\varphi(N) = \#(\mathbb{Z}/N\mathbb{Z})^*$, so $\#H \leq \frac{1}{2}\varphi(N)$, so $\#\{b \notin H\} \geq \frac{1}{2}\varphi(N)$. □

This is encouraging: if N is composite and it is not a pseudoprime to some base, then this can be detected by testing a small number of bases, with high probability. Unfortunately, there exist composite integers which are pseudoprimes to every base.

Definition (Carmichael number)**.** A composite odd $N > 1$ is a **Carmichael number** if it is a Fermat pseudoprime to every base b, $(b, N) = 1$.

Fact. There are infinitely many such numbers (hard theorem). See the example sheet for some properties.

So, we would like to search for stronger tests.

$$a^{p-1} \equiv 1 \pmod{p} \text{ so } a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

In fact, $\equiv \left(\frac{a}{p}\right)$. So, if p is prime, the only square roots of 1 mod p are ± 1.

If N composite, say $N = \prod_{i=1}^{k} p_i^{e_i}$, product of k distinct prime powers, there are 2^k square roots of 1 (mod N) for N odd by the Chinese remainder theorem, as

$$x^2 \equiv 1 \pmod{N} \iff \begin{cases} x^2 \equiv 1 \pmod{p_1^{e_1}} \\ \vdots \\ x^2 \equiv 1 \pmod{p_k^{e_k}} \end{cases}$$

and each of these congruences has 2 solutions.

Definition (Euler pseudoprime)**.** N (an odd composite) is an **Euler pseudoprime** to the base b if

$$b^{\frac{N-1}{2}} \equiv \left(\frac{b}{N}\right) \pmod{N} \qquad (*)$$

Squaring $(*)$ gives that every Euler pseudoprime to base b is also a Fermat pseudoprime (to some base b). Also if N is an Euler pseudoprime to bases b_1 and b_2, then it is also one to base $b_1 b_2$ as

$$(b_1 b_2)^{\frac{N-1}{2}} = b_1^{\frac{N-1}{2}} b_2^{\frac{N-1}{2}} \text{ and } \left(\frac{b_1 b_2}{N}\right) = \left(\frac{b_1}{N}\right)\left(\frac{b_2}{N}\right).$$

So just as for Fermat pseudoprimes:

Proposition 7.2. If N is not an Euler pseudoprime to some base b, then it isn't an Euler pseudoprime to at least $\frac{1}{2}$ of the possible bases.

Proof. Same as in Proposition 7.1 □

Euler pseudoprimes are better than Fermat ones, because

Theorem 7.3. If N is odd, composite, then there is a base b to which N is not an Euler pseudoprime (i.e. there is no analogue of Carmichael numbers for Euler pseudoprimes).

This gives a 'probabilistic' primality test, the Solovay-Strassen probability test: Given $N > 1$ odd,

- Pick $b > 1$ at random. Check $(b, N) = 1$ (if not, N is composite).
- Check whether $b^{\frac{N-1}{2}} \equiv \left(\frac{b}{N}\right) \pmod{N}$ (LHS: write $N-1$ in binary, use repeated squaring, RHS: use quadratic reciprocity law), takes polynomial time.
- If not, then N is certainly composite.
- Otherwise, N is composite with probability $\leq \frac{1}{2}$ (by Proposition 7.2 and Theorem 7.3).
- Repeat for more b's, after t tries, N is prime with probability $1 - \frac{1}{2^t}$.

Proof of Theorem 7.3. There are 2 cases:

a. N **squarefree**, so $N = pm$, p prime, $p \nmid m$, $m \geq 3$. Pick $u \in \mathbb{Z}$ such that $\left(\frac{u}{p}\right) = -1$. Then by the Chinese Remainder Theorem, $\exists b \in \mathbb{Z}$ with $b > 1$ and

$$\begin{aligned} b &\equiv u \pmod{p} \\ b &\equiv 1 \pmod{m} \end{aligned}$$

so

$$\left(\frac{b}{N}\right) = \left(\frac{b}{m}\right)\left(\frac{b}{p}\right) = -1.$$

But $b \equiv 1 \pmod{m} \implies b^{\frac{N-1}{2}} \equiv 1 \not\equiv -1 \pmod{m} \implies b^{\frac{N-1}{2}} \not\equiv -1 \pmod{N}$, so $b^{\frac{N-1}{2}} \not\equiv \left(\frac{b}{N}\right)$, so N is not an Euler pseudoprime to base b.

b. In the other case, some prime p has $p^2 \mid N$. By Chinese Remainder Theorem, $\exists b \in \mathbb{Z}$ with $b \equiv 1 + p \pmod{p^2}$ and $(b, N) = 1$.

$$\begin{aligned} \implies b^{N-1} &\equiv (1+p)^{N-1} \pmod{p^2} \\ &\equiv 1 + p(N-1) \pmod{p^2} \\ &\equiv 1 - p \pmod{p^2} \\ &\not\equiv 1 \pmod{p^2} \end{aligned}$$

So $b^{\frac{N-1}{2}} \not\equiv \pm 1 \pmod{N}$. □

Carry this further. If p prime, $(a, p) = 1$, $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. If $a^{\frac{p-1}{2}} \equiv +1 \pmod{p}$ and $4 \mid p - 1$, then $a^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}$ and so on. This suggests:

Definition (Strong test)**.** Let $N > 1$ be odd, and let $N - 1 = 2^s t$, $s \geq 1$, t odd. Say N passes the **strong test** to base b for $(b, N) = 1$ if either $b^t \equiv 1 \pmod{N}$ or $b^{2^r t} \equiv -1 \pmod{N}$ for some $0 \leq r < s$.

By previous discussion, N prime $\implies$ N passes the strong test (to every base). Say that N is a **strong pseudoprime** to base b if it is composite and passes the strong test (to base b).

Example. Take $N = 65$, $b = 8$. $N - 1 = 64 = 2^6$, so $s = 6$ and $t = 1$.

$8^1 \not\equiv 1 \pmod{N}$ but $8^2 = 64 = -1 \pmod{N}$, so N is a strong pseudoprime to base 8. For $b = 2$, $2^1 \not\equiv 1 \pmod{N}$, and none of $2^2, 2^4, 2^8, 2^{16}, 2^{32}$ are $-1 \pmod{65}$, so N fails the strong test to this base, hence is composite.

Theorem 7.4. If N is a strong pseudoprime to base b, then it is an Euler (hence also Fermat) pseudoprime to base b.

Theorem 7.5. If N composite, then it passes the strong test for at most $\frac{1}{4}\varphi(N)$ bases $b \in \{1, \ldots, N-1\}$, $(b, N) = 1$.

Proof. Omitted in this course. See book by Koblitz. □

Use this as a (probabilistic) primality test (Miller-Rabin test):

- Choose a random base b, $(b, N) = 1$. If N fails the strong test to base b, then it is composite.
- Otherwise, the probability that it is composite is $\leq \frac{1}{4}$.
- Repeat for a total of k bases.

If N passes the strong test for all the bases, then it will be prime with probability $1 - \frac{1}{4^k}$. Hypothetically, can make this deterministic:

Theorem 7.6. If the Generalised Riemann Hypothesis holds, then any composite N fails the strong test for some base $b < 2(\log N)^2$, giving a polynomial time primality test.

In 2002, Agrawal-Kayal-Saxeno discovered a polynomial-time deterministic algorithm which doesn't depend on GRH (or any other unproved assumption). Unfortunately, it's slow for numbers of interest, and takes $\sim (\log N)^{6+\epsilon}$. Upshot: primality testing can be done quickly.

7.1 Factorisation

Factorisation is another story! Take N an odd composite integer. We'd like an algorithm to find a nontrivial factor of N.

The simplest method is 'trial division': check divisibility of N by $3, 5, 7, \ldots$. If $N = pq$, $p, q \approx N^{\frac{1}{2}}$, this will take $\approx N^{\frac{1}{2}}$ steps (but this is good if N happens to have a small factor).

Fermat factorisation

Suppose $N = ab$, $|a - b|$ small. Fermat observed:

$$N = ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

as a, b are both odd. That is, $N + y^2 = x^2$, $x \geq \sqrt{N}$. So try $x = \lfloor\sqrt{N}\rfloor + 1, \lfloor\sqrt{N}\rfloor + 2, \ldots$ and see if $x^2 - N$ is a square, say y^2. If so, $N = (x+y)(x-y)$ gives a factor of N.

Example. Take $N = 200819$,

$$\left\lfloor\sqrt{200819}\right\rfloor = 448$$
$$449^2 - N = 782 \text{ not a square}$$
$$450^2 - N = 1681 = 41^2$$

So $N = 450^2 - 41^2 = 491 \times 409$.

We could have tested $N + y^2$ for squareness, $y = 1, 2, \ldots$, but that would have taken 41 steps.

How many steps does this algorithm take? $x = \lfloor\sqrt{N}\rfloor + t$ will take t steps to get to.

$$N = ab = (x+y)(x-y) \text{ with } x = \frac{a+b}{2} = \lfloor\sqrt{N}\rfloor + t.$$
$$\text{So, } t \approx \frac{a+b}{2} - \sqrt{ab} = \frac{(\sqrt{a} - \sqrt{b})^2}{2} \text{ running time.}$$

If $N = pq, p \approx 10^k, q \approx 2 \times 10^k$, then

$$\frac{(\sqrt{q} - \sqrt{p})^2}{2} \approx \frac{(\sqrt{2} - 1)^2 \cdot 10^4}{2} \approx 0.8 \times 10^{k-1}$$

Better than trial division (10^k) but not by much.

Proposition 7.7. Suppose $x^2 \equiv y^2 \pmod{N}$ and $x \not\equiv \pm y \pmod{N}$. Then the GCDs $(N, x+y)$ and $(N, x-y)$ are both proper divisors of N.

Proof. We treat the case of $x + y$. $(N, x+y) \mid N$ by definition. If $(N, x+y) = N$ then $x \equiv -y \pmod{N}$, a contradiction. If $(N, x+y) = 1$ then $(x+y)(x-y) \equiv 0 \pmod{N}$, hence $x - y \equiv 0 \pmod{N}$, i.e. $x \equiv y \pmod{N}$, a contradiction. □

Finding squares which are congruent mod N is difficult. Instead try to find many integers x_i such that $x_i^2 \equiv c_i \pmod{N}$, where c_i is divisible only by small powers. Then hope to multiply some x_i together to get a solution to $x^2 \equiv y^2 \pmod{N}$.

Lemma 7.8. Let $p_1, \ldots, p_r$ be distinct primes and let $c_1, \ldots, c_k$ be non-zero integers (divisible only by these p_i). Then if $k > r + 1$ there exists a non-empty subset $I \subset \{1, \ldots, k\}$ such that $\prod_{i \in I} c_i$ is a square.

Proof. For any $J \subseteq \{1, \ldots, k\}$ write $c_J = \prod_{i \in J} c_i$ and

$$c_J = (-1)^{\alpha_{J,0}} p_1^{\alpha_{J,1}} \cdots p_r^{\alpha_{J,r}} m_J^2 \text{ where } \begin{cases} m_J \geq 1 \\ \alpha_{J,i} \in \{0, 1\} \end{cases}$$

That is, split c_J into squarefree and squared parts. Observe c_J is a square iff $\alpha_{J,i} = 0 \ \forall i = 0, \ldots, r$.

By the pigeonhole principle, since $k > r+1$, there exist distinct subsets $J, K \subseteq \{1, \ldots, k\}$ such that $\alpha_{J,i} = \alpha_{K,i}$ for each $i = 0, \ldots, r$. It follows that $c_J c_K$ is a square. We also have $c_{J \cap K} \mid c_J$, $c_{J \cap K} \mid c_K$, hence $c_{J \cap K}^2 \mid c_J c_K$. Hence $\frac{c_J c_K}{c_{J \cap K}^2}$ is a square integer, and equals $c_{J \setminus (J \cap K)} c_{K \setminus (J \cap K)} = c_{J \triangle K}$. □

Definition (Factor base)**.** A **factor base** is a set $B = \{-1, p_1, \ldots, p_r\}$ where the p_i are primes. A **B-number** is a positive integer x such that all prime factors of $\langle x^2 \rangle$ lie in B.

If $a \in \mathbb{Z}$, then $\langle a \rangle$ is the unique integer in $(-\frac{N}{2}, \frac{N}{2}]$ such that $\langle a \rangle \equiv a \pmod{N}$.

Here is the 'factor base method' to factor N:

1. Choose a factor base B
2. Generate some B-numbers $x_1, \ldots, x_k$.
3. Find a non-empty subset $I \subseteq \{1, \ldots, k\}$ such that $\prod_{i \in I} \langle x_i^2 \rangle = y^2$ is a square.
4. Then if $x = \prod_{i \in I} x_i$, then $x^2 \equiv y^2 \pmod{N}$. If $x \equiv \pm y \pmod{N}$ then Proposition 7.7 implies we have found a factor of N. Otherwise, find more B-numbers and try again.

How likely is this to work? If $N = \prod_{i=1}^t p_i^{e_i}$ with $e_i \geq 1$ and $p_1, \ldots, p_t$ distinct primes, then the congruence $x^2 \equiv 1 \pmod{p_i^{e_i}}$ has exactly 2 solutions (if $p_i \equiv 2$). By the Chinese Remainder Theorem, the congruence $x^2 \equiv 1 \pmod{N}$ has 2^t solutions. Only two if there

are ± 1. If we apply the factor base method to obtain $x^2 \equiv y^2 \pmod{N}$ then $\left(\frac{x}{y}\right)^2 \equiv 1 \pmod{N}$. As long as $\frac{x}{y}$ is one of the $2^t - 2$ solutions other than ± 1 to $t^2 \equiv 1 \pmod{N}$, we have found a factor of N.

Heuristic: We succeed with probability $1 - \frac{1}{2^{t-1}}$. If $t \geq 2$, we expect this method to eventually factor N.

How do we generate B-numbers, as required by step 2? First guess: try $x_i = \lfloor \sqrt{kN} \rfloor$ or $\lfloor \sqrt{kN} \rfloor + 1$, $k \geq 1$ a small integer.

Then x_i^2 should be close to a multiple of N, hence $\langle x_i^2 \rangle$ should be divisible only by small primes. In practice, generate the x_i first and then choose the factor base B.

Example (Worked example)**.** $N = 1829$. Choose factor base

$$B = \{-1, 2, 3, 5, 7, 11, 13, 17, 19\}$$

x_i	42	43	60	61	74	75	85
$\langle x_i^2 \rangle$	-65	20	-58	63	-11	138	-91
B-number?	$-5 \cdot 13$ ✓	$2^2 \cdot 5$ ✓	$-2 \cdot 29$ ✗	$3^2 \cdot 7$ ✓	-11 ✓	$2 \cdot 3 \cdot 23$ ✗	$-7 \cdot 13$ ✓

Next step: choose some x_i with the property that $\prod \langle x_i^2 \rangle$ is square. By inspection,

$$\begin{aligned} (42 \cdot 43 \cdot 61 \cdot 85)^2 &\equiv (-65 \cdot 20 \cdot 63 \cdot -91) \pmod{N} \\ &\equiv (2 \cdot 3 \cdot 5 \cdot 7 \cdot 13)^2 \pmod{N} \\ \implies 1459^2 &\equiv 901^2 \pmod{N} \end{aligned}$$

We find $(1829, 558) = 31$, $(1829, 2360) = 59$. In this case, $N = 31 \times 59$.

Remark. In general, it need not be the case that $N = (N, x + y)(N, x - y)$.

Computational result: In step 2, we chose B to contain small primes and check whether x_i is a B-number using trial division or using Euclid's algorithm on $\prod_{p_i \in B} p_i$. There is a better way to find B-numbers:

Lemma 7.9. Let $\frac{p_n}{q_n}$ be a convergent in the CF expansion of $\sqrt{N}$. Then $\left|p_n^2 - Nq_n^2\right| \leq 2\sqrt{N}$.

Proof.

$$\begin{aligned} \left|p_n^2 - Nq_n^2\right| &= q_n^2 \left|\sqrt{N} - \frac{p_n}{q_n}\right| \left|\sqrt{N} + \frac{p_n}{q_n}\right| \\ &< q_n^2 \times \left(\frac{1}{q_n q_{n+1}}\right)\left(2\sqrt{N} + \frac{1}{q_n q_{n+1}}\right) \text{ by Theorem 6.4} \\ &= \frac{1}{q_{n+1}}\left(2q_n\sqrt{N} + \frac{1}{q_{n+1}}\right) \\ &< \frac{1}{q_{n+1}}(2q_n + 1)\sqrt{N} \leq 2\sqrt{N} \text{ as } q_{n+1} > q_n. \end{aligned}$$

□

Remark.

(i) So $\langle p_n^2 \rangle \leq 2\sqrt{N}$, so p_n has a good chance of being a B-number.

(ii) Continued fraction factoring method will then work by trying convergents to see if p_n is a B-number. Only need to know p_n and N, so can compute this by $p_{n+1} = a_{n+1}p_n + p_{n-1}$ working mod N.

Example. Take $N = 12403$, and $\sqrt{N} = [111, \overline{2, 1, 2, 2, 7, 1, \ldots}]$, with period 16.

$p_n \pmod N$	111	223	334	891	2116	3309	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	$2 \cdot 83$	$-3 \cdot 13$
		✓			✓		✓

$$\implies (223 \times 2116 \times 5416)^2 \equiv (3^3 \cdot 13)^2 \pmod N$$
$$\implies 11341^2 \equiv 351^2 \pmod N$$

so we have factors $(N, 10990) = 157$ and $(N, 11692) = 79$.

How quick is this? We need to compute enough p_ns to find enough B-numbers, then (step 3 of the previous algorithm) find subsets of these such that

$$\prod_{i \in I} \langle x_i^2 \rangle = c_I = \prod c_i$$

is a square. Writing down all products and using the pigeonhole principle (as in Lemma 7.8) is *much* too slow - there are 2^k numbers, where $k = |I|$. Even if $k \approx \log N$ (which is in practice not enough), this is still $\approx N$.

A far better approach is to look for k-tuples $\gamma = (\gamma_1, \ldots, \gamma_n)$ such that $\prod_{i=1}^k c_i^{\gamma_i}$ is a square. If

$$c_i = (-1)^{a_{i,0}} \prod_{j=1}^r p_j^{a_{ij}} \quad (p_j \in B)$$

this is equivalent to the congruence

$$\forall j = 0, \ldots, r \quad \sum_{i=1}^k \gamma_i \alpha_{ij} \equiv 0 \pmod 2$$

i.e. solving the vector equation $\gamma \cdot (\alpha_{ij}) \equiv 0 \pmod 2$. This can be done with linear algebra (mod 2) by usual Gaussian elimination in $\sim k^3$ operations, and there are faster ways. The final outcome is that this has an expected running time $C \cdot e^{2\sqrt{\log n} \cdot \sqrt{\log \log n}}$. This is asymptotically smaller than any N^ϵ for $\epsilon > 0$, but asymptotically bigger than any $(\log N)^A$ for $A > 0$.

Remark. The 'quadratic sieve' and 'number field sieve' are better still, and they give $e^{\sqrt{\log N} \sqrt{\log \log N}}$ and $e^{b(\log N)^{\frac{1}{3}} (\log \log N)^{\frac{2}{3}}}$ respectively where $b = \left(\frac{64}{9}\right)^{\frac{1}{3}} \approx 1.92$.

For 'special numbers', we can do better:

Pollard's $(p-1)$-method

Suppose $N = pN_0$, $(p, N_0) = 1$ and $p-1$ is a product of small primes. Consider $a^{p-1} - 1 \pmod N$ for $(a, N) = 1$. Then $a^{p-1} - 1 \equiv 0 \pmod p$, and probably $\not\equiv 0 \pmod{N_0}$. Of course, we don't know $p-1$ yet, so can't compute this immediately.

$p = \gcd(a^{p-1} - 1, N)$, but $p-1$ is a product of small primes $\leq m$, say. Then let $k = \mathrm{lcm}(1, \ldots, m)$ (so divisible by all prime powers $q^r \leq m$).

- Choose random $a \geq 2$ with $(a, N) = 1$ (e.g. $a = 2$)
- find $\gcd(a^k - 1, N)$ and hope it is a factor of N.

If all prime powers dividing $p-1$ are $\leq m$, then $a^k \equiv 1 \pmod p$ as $p-1 \mid k$ and unless we are unlucky, $a^k \not\equiv 1 \pmod{N_0}$. (We can compute $(a \mod N)^k$ by repeated squaring.)

Example. Take $N = 540143$. Try $k = \mathrm{lcm}(1, \ldots, m) = 2^3 \cdot 3 \cdot 5 \cdot 7 = 840$. Try $a = 2$. $2^k = 2^{105 \times 8} = (2^{64+32+8+1})^8 \equiv 53047 \pmod N$ and $(540143, 53046) = 421 = p$. N factors as 421×1283. $p - 1 = 420 = 2^2 \cdot 3 \cdot 5 \cdot 7$.

This has two variants:

(1) $(p+1)$-method, i.e. hoping that $p+1$ is a product of small primes. This uses the field with p^2 elements, whose multiplicative group has order $p^2 - 1$.

(2) Elliptic curve method uses 'elliptic curves' instead of finite fields. This has no special restrictions on p, and takes $\sim e^{b\sqrt{\log p}\sqrt{\log\log p}}$, so is better than general methods if p is relatively small, e.g. $N \approx 2^{1000}$, $p \approx 2^{100}$.

Finally Shor's algorithm, sometimes called 'quantum factoring', will factor in polynomial time on a fully-functional quantum computer. So far, the highest number it has factored is 21.