Number Theory

June 2, 2024

Contents

Lectures

Start of

lecture 1

0 Introduction

Number Theory: the study of $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$.

We're interested in questions about:

- Distribution of the primes $p \in \mathbb{Z}$. For example,

  $$\pi(x) = \#\{\text{primes } p \le x\}$$

  How big is $\pi(x)$ as a function of x?

  It turns out that the Riemann hypothesis is equivalent to

  $$\forall x \ge 3, |\pi(x) - \mathrm{li}(x)| \le \sqrt{x} \cdot \log x$$

  where $\mathrm{li}(x)$ is defined as

  $$\mathrm{li}(x) = \int_{t=2}^{x} \frac{1}{\log(t)} \mathrm{d}t$$

- Diophantine equations. For example, Fermat's Last Theorem, which says that if $N \in \mathbb{N} < N \ge 3$ then the equation

  $$X^N + Y^N = Z^N$$

  has no solutions with $X, Y, Z \in \mathbb{Z}$ such that $XYZ = 0$.

- Computation. How can we quickly test whether a given $N \in \mathbb{N}$ is prime? If it's not prime, how can you quickly find its prime factorisation?

We will address all of these themes using techniques coming from IA Numbers and Sets.

1 Primes Numbers and Congruences

Proposition 1.1 (Division algorithm)**.** Let $a, b \in \mathbb{Z}$, $b > 0$. Then there exists a unique pair of $q, r \in \mathbb{Z}$ with $0 \leq r < b$ such that $a = qb + R$.

Proof. Let $S = \{a - qb \mid q \in \mathbb{Z}\}$. We know S contains non-negative elements, so contains a least one, call it r. Then $a = qb + r$. If $r \geq b$, then $r - b \geq 0$, contradicting the minimality of $r \in S$. This shows existence of q, r. If q', r' have the same property, then $qb + r = q'b + r' \implies r - r' = (q' - q)b$. Note that $-b < r - r' < b$. The only multiple of b satisfying this is 0, so $r = r'$ and $q = q'$. □

Notation. If $r = 0$, then $a = qb$. In this case we say that b divides and write $b \mid a$. Otherwise, $b \nmid a$.

Let $a_1, \ldots, a_n \in \mathbb{Z}$ not all 0. Let

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

If $x, y \in I$, $k, l \in \mathbb{Z}$, then $kx + ly \in I$ (this means that I is an ideal of $\mathbb{Z}$).

Lemma 1.2. There exists a unique $d \in \mathbb{N}$ such that $I = d\mathbb{Z} = \{md \mid m \in \mathbb{Z}\}$.

Proof. Let d be the least positive element of I. Then if $a \in I$, we can write $a = qd + r$, $0 \leq r < d$. Then $r = a - qd \in I$. By minimality of d, we must have $r = 0$, hence $a \in d\mathbb{Z}$, and $I \subset d\mathbb{Z}$. Clearly $I \supset d\mathbb{Z}$, hence $I = d\mathbb{Z}$. □

Note that $a_1, \ldots, a_n \in I = d\mathbb{Z}$. Therefore, $d \mid a_i$ for all $i = 1, \ldots, n$. If $e \in \mathbb{N}$, and $e \mid a_i \forall i$, then $e \mid d$.

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

We can use repeated application of the division algorithm to find (a, b). This is *Euclid's algorithm.*

Suppose $a, b \in \mathbb{N}$, $a > b$. Then

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

Claim: we must eventually have $r_{k+2} = 0$. Why? Because $b > r_1 > r_2 > \cdots > r_{k+2} \geq 0$.

Then $(a, b) = r_{k+1}$. Why? Because $(a, b) = (b_1, r_1) = (r_1, r_2) = \cdots = (r_{k+1}, r_{k+2}) = r_{k+1}$.

Corollary 1.3. Let $a, b \in \mathbb{Z}$, not both 0, $c \in \mathbb{Z}$. Then the following are equivalent:

(1) There exist $x, y \in \mathbb{Z}$ such that $xa + yb = c$.

(2) $(a, b) \mid c$.

This is a special case of Lemma 1.2 with $n = 2$, $a_1 = a$, $a_2 = b$. In particular, we can always find $x, y \in \mathbb{Z}$ such that $xa + yb = (a, b)$.

We can use Euclid's algorithm to find such x, y.

Example. $a = 34$, $b = 25$.

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

Therefore $(34, 25) = 1$.

r	x	y
34	1	0
25	0	1
9	1	-1
7	-2	3
2	3	-4
1	-11	15

So $1 = -11 \times 34 + 15 \times 25$.

Definition 1.4. We say $p \in \mathbb{N}$ is prime if $p > 1$ and $\forall b \in \mathbb{N}$, if $b \mid p$ then $b = 1$ or $b = p$.

Lemma 1.5. Let p be a prime number, $a, b \in \mathbb{Z}$. Then if $p \mid (ab)$, then $p \mid a$ or $p \mid b$.

Proof. Suppose $p \mid ab$, $p \nmid a$. We must *show* $p \mid b$.

Consider (a, p). Then $(a, p) \mid p$ so $(a, p) = 1$ or $(a, p) = p$. But $(a, p) \mid a$ so $(a, p) \neq p$, so $(a, p) = 1$. Therefore there exist $x, y \in \mathbb{Z}$ such that $xa + yp = 1$.

Multiply by b: $xab + ypb = b$, so $p \mid b$. □

Theorem 1.6 (Fundamental Theorem of Arithmetic)**.** Let $N \in \mathbb{N}$. Then there is an expression $N = \prod_{i=1}^{k} p_i^{a_i}$ where p_i's are distinct prime numbers, and $a_i \geq 1$ $\forall i = 1, \ldots, k$. Moreover, this expression is unique up to reordering the p_i's.

Proof. Existence: Induction on $N \geq 1$, noting that $N = 1$ has a unique expression as a product of primes. If $N > 1$, either N is prime (in which case we clearly have a representation as a product of primes), or $N = ab$, where $1 < a, b < N$ (and we can use this product to find a representation for N as a product of primes).

Uniqueness: Induction on $N \geq 1$, base case $N = 1$ already treated. If $N > 1$, and we have expressions $N = \prod_{i=1}^k p_i^{a_i} = \prod_{j=1}^l q_j^{b_j}$. Then $p_1 \mid N = \prod_{j=1}^l q_j^{b_j}$. By Lemma 1.5, $p_q \mid q_j$ for some j. Since $p_1 > 1$ and q_j is prime, $p_1 = q_j$. After relabelling, can assume $j = 1$. Then

$$\frac{N}{p_1} = p_1^{a_1 - 1} \prod_{i=1}^k p_i^{a_i} = q_1^{b_1 - 1} \prod_{j=2}^l q_j^{b_j}$$

Now $N/p_1 < N$, so by induction, $k = l$ and $a_i = b_i$ for all i. □

Start of lecture 2

Corollary. Given $m, n \in \mathbb{N}$ with

$$m = \prod_{i=1}^k p_i^{a_i} \qquad n = \prod_{i=1}^k p_i^{b_i} \qquad a_i, b_i \geq 0$$

for some distinct primes p_i, we have

$$(m, n) = \gcd(m, n) = \prod_{i=1}^k p_i^{\min(a_i, b_i)}.$$

In particular,

$$m \mid n \iff (m, n) = m \iff a_i \leq b_i \ \forall i$$

and

$$(m, n) = 1 \iff \min(a_i, b_i) = 0 \ \forall i \iff \nexists \text{ prime } p \text{ such that } p \mid m \text{ and } p \mid n.$$

Definition (Coprime)**.** We say that m and n are *coprime* if $(m, n) = 1$ (which is equivalent to saying that m and n have no common prime factors, by earlier Corollary).

We can compute (m, n) this way, but it's much less efficient than Euclid's algorithm if the prime factorisation of m, n is not already known.

Definition 1.7. An algorithm with input integer $N > 1$ is *polynomial time* if constants $b, c > 0$ such that it always completes after at most $b(\log N)^c$ "elementary operations" (for example adding and multiplying digits in a fixed base).

If an algorithm has inputs $N_1, \ldots, N_k$, it's polynomial time if it completes after $b(\max_i N_i)^c$ operations.

Example.

- Addition and multiplication in the usual way.
- Euclid's algorithm to compute (N_1, N_2) (this is on Example Sheet 1).
- There exists a polynomial time primality test (Agrawal-Kayal-Saxena, 2002).
- What about factorisation? The simplest procedure to factor $N \in \mathbb{N}$ is trial division, i.e. testing each $b \in \mathbb{N}$, $1 < b \leq \sqrt{N}$ to see if $b \mid N$. In the worst case, this requires $\sqrt{N}$ divisions. As $N \to \infty$, $\sqrt{N}$ grows much faster than any power of $\log N$.

  To put this in perspective, suppose $N = pq$ where p, q are 50 digit primes. Suppose we can do 10^{10} divisions per second. To factorise N using trial division would take about $10^{50}/10^{10}$ seconds, which is about 3×10^{32} years.

  There is no known algorithm to factorise integers in polynomial time. Using modern algorithms, it is practical to factor 200 digits. The record is the factorisation of RSA-250 (250 digits). This required thousands of computers working for several months.

Theorem 1.8. There are infinitely many prime numbers.

Proof. Suppose $p_1, \ldots, p_k$ are distinct primes. Let $N = p_1 \cdots p_k + 1$. Then $N > 1$, so it has a prime factor p. We see $p \mid N \implies p \neq p_i \ \forall i$. Therefore there exists at least k distinct primes. □

This is not an efficient way to find primes as it involves factorisation.

One way to generate 50 digit prime numbers is to randomly generate a 50 digit integer and test to see if it is prime. Repeat this until you find a prime number. (Prime Number Theorem tells us how many times we need to do this on average).

For some classes of numbers, there are special (fast) primality tests.

Example. For Mersenne numbers $N = 2^p - 1$ where p is a prime number, there exists Lucas-Lehmer primality test (which is extremely fast). The largest known prime number is the Mersenne number $2^p - 1$ where $p = 82,589,933$ (this has $24,862,048$ decimal digits).

Notation. Fix a *modulus* $N \in \mathbb{N}$. We say $a, b \in \mathbb{Z}$ are congruent modulo N if $N \mid (a - b)$ and write $a \equiv b \pmod{N}$.

Congruence modulo N is an equivalence relation on $\mathbb{Z}$ with classes $a+N\mathbb{Z}$. The operation $(a+n\mathbb{Z})+(b+N\mathbb{Z}) = (a+b)+n\mathbb{Z}$ and $(a+N\mathbb{Z})(b+N\mathbb{Z}) = ab+N\mathbb{Z}$ are well-defined. (Alternatively, $N\mathbb{Z} \trianglelefteq \mathbb{Z}$ is an ideal, $\mathbb{Z}/N\mathbb{Z}$ is the quotient ring).

Lemma 1.9. Let $a \in \mathbb{Z}$. The following are equivalent:

(1) $(a, N) = 1$

(2) $\exists b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{N}$

(3) $a + N\mathbb{Z}$ generates $(\mathbb{Z}/N\mathbb{Z}, +)$ (the additive group of congruence classes modulo N)

Proof.

(1) $\implies$ (2) If $(a, N) = 1$, there exists $x, y \in \mathbb{Z}$ such that $xa + yN = 1$, i.e. $xa \equiv 1 \pmod{N}$.

(2) $\implies$ (1) If there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{N}$, then there exists $k \in \mathbb{Z}$ such that $ab - 1 = kN$, i.e. $ab - kN = 1$, hence $(a, N) = 1$.

(2) $\iff$ (3) $1+N\mathbb{Z}$ generates $(\mathbb{Z}/N\mathbb{Z}, +)$ as $\underbrace{(1+N\mathbb{Z}) + \cdots + (1+N\mathbb{Z})}_{b \text{ times}}$ equals $b+N\mathbb{Z}$.

So $a+N\mathbb{Z}$ is a generator if and only if it generates $1+N\mathbb{Z}$, which happens if and only if there exists $b \in \mathbb{N}$ such that $\underbrace{(a+N\mathbb{Z}) + \cdots + (a+N\mathbb{Z})}_{b \text{ times}} = 1 + N\mathbb{Z}$. This happens if and only if there exists b with $ab \equiv 1 \pmod{N}$. $\square$

Notation. If $N > 1$, we write $(\mathbb{Z}/N\mathbb{Z})^\times$ for the group of congruence classes of a modulo N such that $(a, N) = 1$, under multiplication. We sometimes call $(\mathbb{Z}/N\mathbb{Z})^\times$ the group of units modulo N.

We also write $\phi(N) := \#(\mathbb{Z}/N\mathbb{Z})^\times$ (we call this *Euler's totient function*).

Note that $\phi(N) \leq N - 1$, with equality if and only if for all $b \in \mathbb{N}$ with $1 \leq b \leq N - 1$, we have $(b, N) = 1$. This happens if and only if N is prime.

Corollary 1.10. Let G be a cyclic group of order $N > 1$. Then G contains $\phi(N)$ elements of order N.

Proof. G is isomorphic as a group to $(\mathbb{Z}/N\mathbb{Z}, +)$. The elements of order N are exactly the generators of the group. By Lemma 1.9, these are exactly the congruence classes $a + N\mathbb{Z}$ with $(a, N) = 1$. There are $\phi(N)$ of these, by definition. □

Start of lecture 3

Proposition 1.11 (Euler-Fermat Theorem)**.** If $a, N \in \mathbb{Z}$, $N > 1$, $(a, N) = 1$, then

$$a^{\phi(N)} \equiv 1 \pmod{N}$$

Proof. Lagrange's theorem says: if G is a finite group, $g \in G$, then $\underbrace{g \cdot g \cdots g}_{\#G \text{ times}} = e$. We take $G = (\mathbb{Z}/N\mathbb{Z})^\times$, $g = a + N\mathbb{Z}$, so $a^{\phi(N)} \equiv 1 \pmod{N}$. □

Corollary 1.12 (Fermat's Little Theorem)**.** If p is a prime number, $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.

Proof. If $p \mid a$, then $a^p \equiv 0 \equiv a \pmod{p}$, so done.

If $p \nmid a$, then $(a, p) = 1$, so by Euler-Fermat Theorem $a^{p-1} \equiv 1 \pmod{p}$, so $a^p \equiv a \pmod{p}$. □

Example. Can we find $x \in \mathbb{Z}$ such that $x \equiv 7 \pmod{10}$ and $x \equiv 3 \pmod{13}$? In other words, is the intersection $(7 + 10\mathbb{Z}) \cap (3 + 13\mathbb{Z})$ non-empty?

We can write down a solution if we can find $u, v \in \mathbb{Z}$ such that

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

because then $x = 7u + 3v$ is a solution. As $(10, 13) = 1$, we can find $r, s \in \mathbb{Z}$ such that $10r + 13s = 1$. Then $10r + 13s = 1 \implies 10r = 1 - 13s$, so can take $v = 10r$ and $13s = 1 - 10r$, so can take $u = 13s$.

We can take $r = 4$, $s = -3$. Then $v = 40$, $u = -39$, so a solution is $x = -39 \times 7 + 40 \times 3$.

Theorem 1.13 (Chinese Remainder Theorem)**.** Let $m_1, \dots, m_k \in \mathbb{N}$ be pairwise coprime, i.e. such that $(m_i, m_j) = 1$ if $i \neq j$. Let $M = m_1 \cdots m_k$ and suppose again $a_1, \dots, a_k \in \mathbb{Z}$.

Then there exists $x \in \mathbb{Z}$ such that x satisfies

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

Moreover, any other solution is congruent to $x \pmod{M}$.

Proof. If x is a solution, then $x + rM$ is also a solution for any $r \in \mathbb{Z}$. Why? $m_i \mid M$, so $x + rM \equiv x \pmod{m_i}$. If y is another solution, then $x \equiv y \pmod{m_i}$ for all $i = 1, \dots, k$. So $m_i \mid (x - y)$, hence $M \mid (x - y)$ as m_i are pairwise coprime (so they have no prime factors in common). So $x \equiv y \pmod{M}$.

To find a solution, let's define $M_i = \frac{M}{m_i} = \prod_{j \neq i m_j}$. Since m_j are pairwise coprime, $(m_i, M_i) = 1$, there exist r_i, s_i such that $r_i m_i + s_i M_i = 1$. Then

$$\begin{aligned} s_i M_i = &\equiv 1 \pmod{m_i} \\ &\equiv 0 \pmod{M_i} \\ &\equiv 0 \pmod{m_j} && \text{(for } j \neq i \text{, as } m_j \mid M_i) \end{aligned}$$

We take

$$x = \sum_{i=1}^{k} s_i M_i a_i$$

Then

$$x \equiv \sum_{i=1}^{k} s_i M_i a_i \pmod{m_j} \equiv s_j M_j a_j \equiv a_j \pmod{m_j}$$ □

Theorem 1.14. Let $m_1, \dots, m_k \in \mathbb{N}$ be pairwise coprime, $M = \prod_{i=1}^{k} m_i$. Then the map

$$\begin{aligned} \theta : \mathbb{Z}/M\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \\ a + M\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, \dots, a + m_k\mathbb{Z}) \end{aligned}$$

is a ring isomorphism, i.e. a bijection that preserves addition and multiplication.

Proof.

$$\theta(a + b + M\mathbb{Z}) = \theta(a + M\mathbb{Z}) + \theta(b + M\mathbb{Z})$$
$$\theta(ab + M\mathbb{Z}) = \theta(a + M\mathbb{Z})\theta(b + M\mathbb{Z})$$

because addition and multiplication are defined pointwise on RHS.

θ being bijective is exactly the content of the Chinese Remainder Theorem. □

Corollary 1.15. Let $m_1, \dots, m_k$ be pairwise coprime integers such that $m_i > 1$ for all $i = 1, \dots, k$, $M = \prod_{i=1}^{k} m_i$. Then there's a group isomorphism

$$(\mathbb{Z}/M\mathbb{Z})^\times \equiv (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})^\times$$

Proof. Restrict θ from Theorem 1.14 to the group of elements which have a multiplicative inverse. Just check that the image is what we expect. □

We will now show that if p is a prime, then $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group. Consequence of this and Corollary 1.15: if $N \in \mathbb{N}$ is odd, $N > 1$, then N has at least 2 distinct prime factors if and only if $(\mathbb{Z}/N\mathbb{Z})^\times$ is not cyclic.

Definition 1.16 (Multiplicative Function)**.** A function $f : \mathbb{N} \to \mathbb{C}$ is *multiplicative* if $\forall m, n \in \mathbb{N}$ such that $(m, n) = 1$, $f(mn) = f(m)f(n)$.

We say f is *totally multiplicative* if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$.

Example. For example $f(n) = n^k$, $k \in \mathbb{N}$ is totally multiplicative, while ϕ is not totally multiplicative (for example $\phi(4) = 2$, but $\phi(2)\phi(2) = 1^2 \neq 2$). The next lemma will show that we can extend ϕ to a multiplicative function.

Lemma 1.17. ϕ is multiplicative if we extend ϕ to $\mathbb{N}$ by setting $\phi(1) = 1$.

Proof. Let $m, n \in \mathbb{N}$, $(m, n) = 1$, $m, n > 1$. Then there's an isomorphism

$$(\mathbb{Z}/mn\mathbb{Z})^\times \equiv (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

Note $\phi(mn)$ is equal to the cardinality of the LHS, and $\phi(m)\phi(n)$ is equal to the cardinality of the RHS. □

Proposition 1.18. Let $f : \mathbb{N} \to \mathbb{C}$ be a multiplicative function, and define $g : \mathbb{N} \to \mathbb{C}$ by $g(n) = \sum_{d|n} f(d)$ ($\sum_{d|n}$ means sum over *positive* divisors of n, including 1 and n).

Proof. Let $m, n \in \mathbb{N}$, $(m, n) = 1$. Then $g(mn) = \sum_{d|mn} f(d)$. Since $(m, n) = 1$, each $d \mid mn$ admits a unique expression $d = d_1 d_2$, where $d_1 \mid m$, $d_2 \mid n$. So

$$\begin{aligned} g(mn) &= \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) \\ &= \left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right) \\ &= g(m) g(n) \end{aligned}$$

□

Example. If $f(n) = n^k$, then $g(n) = \sum_{d|n} d^k =: \sigma_k(n)$ is multiplicative.

Start of

lecture 4

Proposition 1.19 (totient function formulae)**.**

(1) If p is a prime number, $k \in \mathbb{N}$, $\phi(p^k) = p^k = k^{k-1}$.

(2) If $N \in \mathbb{N}$, then

$$\phi(N) = N \prod_{p \mid N \text{ prime}} \left(1 - \frac{1}{p}\right)$$

(3) If $N \in \mathbb{N}$, $\sum_{d|N} \phi(d) = N$.

Proof.

(1)
$$\begin{aligned}\phi(p^k) &= \#\{1 \leq a \leq p^k \mid (a,p) = 1\} \\ &= \#\{1 \leq a \leq p^k\} - \#\{1 \leq a \leq p^k \mid p \mid a\} \\ &= p^k - p^{k-1}\end{aligned}$$

(2) Assume $N > 1$, and factorise $N = \prod_{i=1}^r p_i a^i$, $a_i \geq 1$, p_i distinct primes. Since ϕ is multiplicative,

$$\phi(N) = \prod_{i=1}^r \phi(p_i^{a_i}) = \prod_{i=1}^r p_i^{a_i} \left(1 - \frac{2}{p_i}\right) = N \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

(3) We know $f(N) = \sum_{d|N} \phi(d)$ is multiplicative. Want to show $f(N) = N$. It's enough to check this equality when $N = p^k$ is a prime power ($k \geq 1$).

$$f(p^k) = \sum_{i=0}^k \phi(p^i) = (p^k - p^{k-1}) + (p^{k-1} - p^{k-2}) + \cdots + (p-1) + 1 = p^k \qquad \square$$

Polynomial Congruences

If $N \in \mathbb{N}$, a polynomial $f(X)$ with coefficients in $\mathbb{Z}/N\mathbb{Z}$ is a formal linear combination

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

of powers of X, $a_i \in \mathbb{Z}/N\mathbb{Z}$. Two polynomials are equal if their coefficients are equal (so for example $X = X + 0 \cdot X^2$).

We write $\mathbb{Z}/N\mathbb{Z}[X]$ for the set of polynomials with coefficients in $\mathbb{Z}/N\mathbb{Z}$. You can add and multiply these in the usual way, which gives this a ring structure.

If $a \in \mathbb{Z}/N\mathbb{Z}$,

$$f(a) =: a_n a^n + \cdots + a_1 a + a_0 \in \mathbb{Z}/N\mathbb{Z}.$$

The *solutions* to $f(X) = 0$ in $\mathbb{Z}/N\mathbb{Z}$ are the $a \in \mathbb{Z}/N\mathbb{Z}$ such that $f(a) \equiv \pmod{N}$. For example $X^2+2 = 0$ in $\mathbb{Z}/5\mathbb{Z}$ has no solutions, while $X^3+1 = 0$ has 3 solutions in $\mathbb{Z}/7\mathbb{Z}$: 3, 5 and 6 modulo 7. The equation $X^2 - 1 = 0$ has 4 solutions in $\mathbb{Z}/8\mathbb{Z}$: 1, 3, 5 and 7 modulo 8. Note that in this last case, the congruence has more than the "expected" number of solutions (i.e. degree of $f(X) = 2$ in this case). This can happen only when the modulus is not prime.

Theorem 1.20 (Lagrange's Theorem)**.** Let p be a prime number,

$$f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}/p\mathbb{Z}[X]$$

with $a_n \not\equiv 0 \pmod{p}$. Then the equation $f(X) = 0$ has at most n solutions in $\mathbb{Z}/p\mathbb{Z}$.

Proof. Induction on $n \geq 0$. If $n = 0$, $f(X) = a_0 \not\equiv \pmod{p}$. Want to solve $a_0 \equiv \pmod{p}$. This has 0 solutions as desired.

Suppose $n > 0$. Assume that $f(X) = 0$ has at least 1 solution, say $a \in \mathbb{Z}/p\mathbb{Z}$ (and if there are no solutions, then we are already done). Note if $j > 0$, then

$$X^j - a^j = (X - a)(X^{j-1} + aX^{j-2} + \cdots + a^{j-1})$$

so

$$f(X) = f(X) - f(A) = \sum_{j=1}^{n} a_j (X^j - a^j) = (X - a) \underbrace{\sum_{j=1}^{n} a_j (X^{j-1} + aX^{j-2} + \cdots + a^{j-1})}_{=:g(X)}$$

Note that $g(X)$ has leading term $a_n X^{n-1}$. Suppose $b \in \mathbb{Z}/p\mathbb{Z}$ is a solution to $f(X) = 0$ distinct from a. Then $0 \equiv f(b) \equiv (b - a)g(b) \pmod{p}$. Since p is prime and $a \not\equiv b \pmod{p}$, $b-a$ has a multiplicative inverse modulo p. So $g(b) \equiv 0 \pmod{p}$. By induction, we know $g(X) = 0$ has at most $n - 1$ solutions in $\mathbb{Z}/p\mathbb{Z}$. Hence $f(X) = 0$ has at most n solutions. □

Theorem 1.21. Let p be a prime number. Then $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p - 1$.

Proof. We know $\#(\mathbb{Z}/p\mathbb{Z})^\times = \phi(p) = p-1$. From Proposition 1.19, we know

$$p - 1 = \sum_{d \mid p-1} \phi(d).$$

We know that if $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ then order of a divides $p-1$ (Lagrange's theorem from group theory). If N_d denotes the number of elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ of order d, then

$$\sum_{d \mid p-1} N_d = p - 1$$

We want to show $N_{p-1} > 0$. Suppose for contradiction that $N_{p-1} = 0$. Note

$$\sum_{d \mid p-1} N_d = p - 1 = \sum_{d \mid p-1} \phi(d).$$

We know $\phi(p-1) > 0$. If $N_{p-1} = 0$, then we must have $N_d > \phi(d)$ for some $d \mid p-1$. Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times)$ be some element of this order d. Consider the cyclic subgroup $\langle a \rangle = \{1, a, \dots, a^{d-1}\} = (\mathbb{Z}/p\mathbb{Z})^\times$. It's cyclic of order d, so has $\phi(d)$ elements of order d (Corollary 1.10). We know $N_d > \phi(d)$, so there must exist $b \in (\mathbb{Z}/p\mathbb{Z})^\times$ of order d, not contained in this subgroup. Claim: $\{1, a, \dots, a^{d-1}, b\}$ are $d+1$ solutions to $X^d - 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$. This is clearly true for b, and for the powers of a, note $(a^i)^d \equiv a^{id} \equiv (a^d)^i \equiv 1^i \equiv 1 \pmod{p}$. But this contradicts Theorem 1.20 (Lagrange's Theorem). □

Definition 1.22 (primitive root)**.** Let p be a prime number, $a \in \mathbb{Z}$. We say that a is a *primitive root modulo* p if $a + N\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$ generates the group.

The theorem says that primitive roots always exist.

Example. For $p = 7$, one can check that 2 is not a primitive root, while 3 is.

Start of

lecture 5

Example. Is 2 a primitive root modulo $p = 19$? $\phi(p) = 18$, so if d is the order of 2 modulo 19, then $d \mid 18$ and

$$d = 18 \iff 2 \text{ is a primitive root modulo } 19$$

The divisors of 18 are 1, 3, 9, 2, 6 and 18. So 2 is a primitive root if and only if $2^6 \not\equiv 1 \pmod{19}$ and $2^9 \not\equiv 1 \pmod{19}$.

$$\begin{aligned} 2^4 = 16 &\equiv -3 \pmod{19} \\ 2^6 \equiv -12 &\not\equiv 1 \pmod{19} \\ 2^9 = 8 \times 2^6 \equiv 56 \equiv -1 &\not\equiv 1 \pmod{19} \end{aligned}$$

So 2 is a primitive root modulo p.

Remark. If p is a prime number, $a \in \mathbb{Z}$, then a is a primitive root modulo p if and only if

$$a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p} \qquad \forall \text{prime divisors } q \text{ of } p-1$$

Checking this requires knowing the prime factorisation of $p - 1$.

There is no known polynomial time algorithm for finding a primitive root modulo a given prime p. One can show that, assuming GRH (generalised Riemann hypothesis), there exists $c > 0$ such that for any prime number p, there exists $a \in \mathbb{Z}$, $1 \le a \le c(\log p)^6$ such that a is a primitive root modulo p.

Theorem 1.23. Let p be an odd prime, $k \in \mathbb{N}$. Then $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic.

Remark. The corresponding statement is false for $p = 2$, on $(\mathbb{Z}/8\mathbb{Z})^\times \simeq C_2 \times C_2$ which is not cyclic.

Lemma 1.24. Let p be an odd prime, $k \in \mathbb{N}$, $x, y \in \mathbb{Z}$. Then:

(1) If $x \equiv 1 + p^k y \pmod{p^{k+1}}$, then $x^p \equiv 1 + p^{k+1} y \pmod{p^{k+2}}$.

(2) $(1 + py)^{p^k} \equiv 1 + p^{k+1} y \pmod{p^{k+2}}$.

Proof. (1) Note that $x = 1 + p^k y + p^{k+1} z$ for some $z \in \mathbb{Z}$. Then

$$x^p = (1 + p^k y)^p + \sum_{j=1}^{p} \binom{p}{j} (1 + p^k y)^{p-j} (p^{k+1} z)^j$$

If $1 \leq j \leq p-1$, then $p \mid \binom{p}{j}$, so $p \cdot p^{k+1} \mid \binom{p}{j}(p^{k+1}z)^j$. For $j = p$, $(p^{k+1}z)^p = p^{pk+p}z^p$. Since $pk + p \geq k + 2$, $p^{k+2} \mid (p^{k+1}z)^p$. So each term of the sum is $0 \pmod{p^{k+2}}$, so $x^p \equiv (1 + p^k y)^p \pmod{p^{k+2}}$. Now we compute:

$$(1 + p^k y)^p = 1 + p^{k+1} y + \sum_{j=2}^{p} \binom{p}{j} (p^k y)^j$$

If $2 \leq j \leq p-1$, then $p \mid \binom{p}{j}$, so $p^{2k+1} \mid \binom{p}{j}(p^k y)^j$. We have $2k+1 \geq k+2 \iff k \geq 1$, so $p^{k+2} \mid \binom{p}{j}(p^k y)^j$. $(p^k y)^p = p^{pk} y^p$. We have $pk \geq k + 2 \iff (p-1)k \geq 2$. We're assuming p is odd, so $p - 1 \geq 2$, so $(p-1)k \geq 2$. So all the terms in the sum are divisible by p^{k+2}, so $x^p \equiv 1 + p^{k+1} y \pmod{p^{k+2}}$ as desired.

(2) Apply part (1) k times to $1 + py, (1 + py)^p, \ldots$. □

Lemma 1.25. Let p be an odd prime, $k \geq 2$, $a \in \mathbb{Z}$. If a is a primitive root modulo p but $a^{p-1} \not\equiv 1 \pmod{p^2}$, then a generates $(\mathbb{Z}/p^k\mathbb{Z})^\times$.

Proof. Let d be the order of $a \in (\mathbb{Z}/p^k\mathbb{Z})^\times$. Then $d \mid \phi(p^k) = p^{k-1}(p-1)$. We know $a^d \equiv 1 \pmod{p^k} \implies a^d \equiv 1 \pmod{p}$, so $p - 1 \mid d$ (since a is a primitive root modulo p). We must have $d = p^j(p-1)$ for some $0 \leq j \leq k-1$. Need to show $j = k-1$. We can write $a^{p-1} = 1 + py$ with $y \in \mathbb{Z}$, $(p, y) = 1$ (as $a^{p-1} \not\equiv 1 \pmod{p^2}$). So

$$\begin{aligned} a^{(p-1)p^{k-2}} = (1 + py)^{p^{k-2}} &\equiv 1 + p^{k-1} y \pmod{p^k} \qquad \text{by Lemma 1.24(2)} \\ &\not\equiv 1 \pmod{p^k} \end{aligned}$$

So $d \nmid (p-1)p^{k-2}$. This forces $d = (p-1)p^{k-1}$, so a generates $(\mathbb{Z}/p^k\mathbb{Z})^\times$. □

We can now prove Theorem 1.23 (i.e. $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic when p is odd):

Proof. We can assume $k \geq 2$. Let $a \in \mathbb{Z}$ be a primitive root modulo p. If $a^{p-1} \not\equiv 1 \pmod{p^2}$, then $a \pmod{p^k}$ generates $(\mathbb{Z}/p^k\mathbb{Z})^\times$, and we're done. So suppose $a^{p-1} \equiv 1 \pmod{p^2}$, and let $b = (1 + p)a$.

Claim: $b \pmod{p^k}$ generates $(\mathbb{Z}/p^k\mathbb{Z})^\times$.

Since $b \equiv a \pmod p$, b is a primitive root modulo p. By Lemma 1.25, the claim is true if $b^{p-1} \not\equiv 1 \pmod{p^2}$, or equivalently if $b^p \not\equiv b \pmod{p^2}$. We compute

$$b^p = (1+p)^p a^p \equiv a^p \pmod{p^2}$$

We're assuming that $a^p \equiv a \pmod{p^2}$, so $b^p \equiv a \pmod{p}^2$. By construction we have $b \not\equiv a \pmod{p}^2$, so $b^p \not\equiv b \pmod{p^2}$, so the claim is true. $\square$

Example. In last lecture, we saw that 2 is not a primitive root modulo 7, but 3 is. Does $3 \pmod{7^k}$ generate $(\mathbb{Z}/7^k\mathbb{Z})^\times$ for all $k > 1$? This is true if and only if $3^6 \not\equiv 1 \pmod{49}$.

$$3^4 = 81 = 100 - 19 = 98 + 2 - 19 \equiv -17 \pmod{49}$$

$17 \times 3 = 51 \equiv 2 \pmod{49}$, so $3^5 \equiv -2 \pmod{49}$ so $3^6 \equiv -6 \not\equiv 1 \pmod{49}$. So $3 \pmod{7^k}$ does generate the group for all $k \geq 1$.

Remark. What happens when $p = 2$? Lemma 1.24(1) fails when $p = 2$, $k = 1$ ($(1+2)^2 \equiv 1 \pmod 8$). It does hold when $k \geq 2$. Using this, you can show that

$$\ker((\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times)$$

is cyclic when $k \geq 2$, of order 2^{k-2}. Using this one can show that there's an isomorphism $(\mathbb{Z}/2^k\mathbb{Z})^\times \simeq C_{2^{k-2}} \times C_2$, with generators $5, -1$ modulo 2^k.

Start of

lecture 6

2 Quadratic Reciprocity

Definition 2.1 (Quadratic residue)**.** Let p be a prime, $a \in \mathbb{Z}$. We say $a \bmod p$ is a *quadratic residue* if the equation $X^2 = a$ has a solution in $\mathbb{Z}/p\mathbb{Z}$. If there's no solution, we say a is a *quadratic non-residue.*

Example. $p = 7$:

x	0	1	2	3	4	5	6
$x^2 \bmod 7$	0	1	4	2	2	4	1

So the quadratic residues modulo 7 are 1, 2 and 4. The non-residues are 3, 5 and 6.

Lemma 2.2. If p is an odd prime, then there are $\frac{p-1}{2}$ quadratic residue modulo p, and $\frac{p-1}{2}$ non-residues.

Proof. Consider $\theta : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$, $\theta(x) = x^2$. Want to show that the image of θ contains exactly $\frac{p-1}{2}$ elements. Enough to show that each fibre of θ contains exactly 2 elements. If $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, then $\theta(x) = \theta(-x)$. If $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\theta(x) = x^2 = y^2 = \theta(y)$, then $(x + y)(x - y) \equiv 0 \pmod p$, so $x \equiv y \pmod p$ or $x \equiv -y \pmod p$, as p is prime, so every fibre contains exactly 2 elements as desired. □

Notation (Legendre symbol)**.** If p is an odd prime, $a \in \mathbb{Z}$, then the *Legendre symbol* is

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

Proposition 2.3 (Euler's Criterion)**.** If p is an odd prime, $a \in \mathbb{Z}$, then $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$.

Proof. If $p \mid a$, this holds by definition, so let's assume $p \nmid a$. Then Euler-Fermat Theorem says

$$(a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1 \pmod p \implies a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$$

If a is a quadratic residue, then $a \equiv x^2$ for some $x \in \mathbb{Z}$, hence $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$. So $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$ in this case.

By Lagrange's Theorem, the equation $X^{\frac{p-1}{2}} = 1$ has at most $\frac{p-1}{2}$ solutions in $\mathbb{Z}/p\mathbb{Z}$. We've shown that the quadratic residues give $\frac{p-1}{2}$ solutions. If a is a quadratic non-residue, then we must have $a^{\frac{p-1}{2}} \equiv -1 \pmod p$, i.e. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$. □

Corollary 2.4. If $a, b \in \mathbb{Z}$, then

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

Proof. For p odd, 0, 1 and -1 lie in distinct congruence classes modulo p. So it's enough to show that LHS $\equiv$ RHS $\pmod p$. But

$$\text{LHS} \equiv (ab)^{\frac{p-1}{2}} \pmod p, \qquad \text{RHS} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod p$$ □

Remark. If we use QR to represent quadratic residues and NQR to represent quadratic non-residues, we have

$$\text{QR} \times \text{QR} = \text{QR}, \qquad \text{NQR} \times \text{NQR} = \text{QR}, \qquad \text{NQR} \times \text{QR} = \text{NQR}.$$

Corollary 2.5.

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

Notation. If p is an odd prime, $a \in \mathbb{Z}$, then $\langle a \rangle$ denotes the unique integer such that $a \equiv \langle a \rangle \pmod p$ and $-\frac{p}{2} < \langle a \rangle \frac{p}{2}$. (So $\langle a \rangle \in \left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \dots, \frac{p-1}{2}\right\}$).

Lemma 2.6 (Gauss's Lemma)**.** Let p be an odd prime, $a \in \mathbb{Z}$, $p \nmid a$. Then $\left(\frac{a}{p}\right) = (-1)^{\mu}$, where

$$\mu = \#\{i \in \mathbb{Z} \mid 0 < i < \frac{p}{2} \text{ and } \langle ai \rangle < 0\}.$$

Inspiration for proof: One way of proving Fermat's Little Theorem is to consider the action of $\times a$ on $1, \ldots, p-1 \bmod p$. Multiplication by a will permute these, so

$$\begin{aligned} \prod_{i=1}^{p-1} \equiv \prod_{i=1}^{p-1} ai \pmod p &\implies (p-1)! \equiv a^{p-1}(p-1)! \pmod p \\ &\implies a^{p-1} \equiv 1 \pmod p \end{aligned}$$

Proof. We consider

$$\prod_{i=1}^{\frac{p-1}{2}} ai = a^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} i = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$

We also have

$$\prod_{i=1}^{\frac{p-1}{2}} ai \equiv \prod_{i=1}^{\frac{p-1}{2}} \langle ai \rangle \pmod p.$$

For each $i = 1, \ldots, \frac{p-1}{2}$, there's a unique sign $\varepsilon_i \in \{\pm 1\}$ such that $\varepsilon_i \langle ai \rangle > 0$.

Claim: The set $\left\{\varepsilon \langle ai \rangle \mid i = 1, \ldots, \frac{p-1}{2}\right\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$.

Proof of claim: LHS $\subset$ RHS as $0 < \varepsilon_i \langle ai \rangle < \frac{p}{2}$. We need to show that if $i \neq j$, then $\varepsilon_i \langle ai \rangle \neq \varepsilon_j \langle aj \rangle$. If $\varepsilon_i \langle ai \rangle = \varepsilon_j \langle aj \rangle$, then

$$ai \equiv \varepsilon_i \varepsilon_j a_j \pmod p \implies i \equiv \pm j \pmod p.$$

By assumption, $i, j \in \left\{1, \ldots, \frac{p-1}{2}\right\}$. If $i \equiv \pm j \pmod p$ then we must have $i \equiv j \pmod p$, so $i = j$.

Putting this together, we find

$$\begin{aligned} \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i \langle ai \rangle &\equiv \prod_{i=1}^{\frac{p-1}{2}} (\varepsilon_i) \cdot \prod_{i=1}^{\frac{p-1}{2}} ai \\ &= \prod_{i=1}^{\frac{p-1}{2}} (\varepsilon_i) \cdot a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \end{aligned}$$

and

$$\prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i \langle ai \rangle \equiv \prod_{i=1}^{\frac{p-1}{2}} i \equiv \left(\frac{p-1}{2}\right)! \pmod p \implies \left(\prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i\right) \cdot a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

$$\implies \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i \equiv \left(\frac{a}{p}\right) \pmod p$$

$$\implies (-1)^\mu = \left(\frac{a}{p}\right) \qquad \square$$

Example. We can compute $\left(\frac{-1}{p}\right)$ using Gauss's Lemma: $\left(\frac{-1}{p}\right) = (-1)^\mu$ where

$$\mu = \#\left\{1 \le i \le \frac{p-1}{2} \;\middle|\; \langle -i \rangle < 0\right\} = \#\left\{1 \le i \le \frac{p-1}{2} \;\middle|\; -i < 0\right\} = \frac{p-1}{2}$$

Example. Next compute $\left(\frac{2}{p}\right) = (-1)^\mu$, where

$$\mu = \#\left\{0 < i < \frac{p}{2} \;\middle|\; \langle 2i \rangle < 0\right\}.$$

If $i \in \mathbb{Z}$ and $0 < i < \frac{p}{4}$, then $0 < 2i < \frac{p}{2}$, so $\langle 2i \rangle = 2i > 0$. If $i \in \mathbb{Z}$ and $\frac{p}{4} < i < \frac{p}{2}$, then $\frac{p}{2} < 2i < p$, so $-\frac{p}{2} < 2i - p < 0$, so $\langle 2i \rangle = 2i - p < 0$.

So

$$\mu = \#\left\{i \in \mathbb{Z} \;\middle|\; \frac{p}{4} < i < \frac{p}{2}\right\} = \left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor$$

where if $x \in \mathbb{R}$, $\lfloor x \rfloor = \sup\{n \in \mathbb{Z} \mid n \le x\}$. Then $(-1)^\mu = \left(\frac{2}{p}\right)$ depends on $p \bmod 8$.

p	$\frac{p}{2}$	$\lfloor \frac{p}{2} \rfloor$	$\frac{p}{4}$	$\lfloor \frac{p}{4} \rfloor$	μ	$(-1)^\mu$
$8k+1$	$4k+\frac{1}{2}$	$4k$	$2k+\frac{1}{4}$	$2k$	$2k$	1
$8k+3$	$4k+\frac{3}{2}$	$4k+1$	$2k+\frac{3}{4}$	$2k$	$2k+1$	-1
$8k+5$	$4k+\frac{5}{2}$	$4k+2$	$2k+\frac{5}{4}$	$2k+1$	$2k+1$	-1
$8k+7$	$4k+\frac{7}{2}$	$4k+3$	$2k+\frac{7}{4}$	$2k+1$	$2k+2$	1

$$\implies \left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1, 7 \pmod 8 \\ -1 & p \equiv 3, 5 \pmod 8 \end{cases}$$

Start of lecture 7

Example. If $a = 3$, then for $p > 3$,

$$\mu = \#\left\{b \in \mathbb{Z} \;\middle|\; 0 < b < \frac{p}{2}, \langle 3b \rangle < 0\right\}$$

If $0 < b < \frac{p}{6}$, $0 < 3b < \frac{p}{2}$, so $\langle 3b \rangle = 3b > 0$. If $\frac{p}{6} < b\frac{p}{3}$, $\frac{p}{2}3b > p$, $-\frac{p}{2} < 3b - p < 0$, so $\langle 3b \rangle = 3b - p < 0$. If $\frac{p}{3} < b < \frac{p}{2}$, $p < 3b < \frac{3p}{2}$, $0 < 3b - p < \frac{p}{2}$, so $\langle 3b \rangle = 3b - p > 0$. So

$$\mu = \#\left\{b \in \mathbb{Z} \;\middle|\; \frac{p}{2} < b < \frac{p}{3}\right\}$$

In this case, $(-1)^\mu = \left(\frac{3}{p}\right)$ depends only on $p \bmod 12$. In general, if $a \in \mathbb{Z}$, $p \nmid a$, $b \in \mathbb{Z}$, then there exists $c \in \mathbb{Z}$ such that $-\frac{p}{2} < ab - pc < \frac{p}{2}$. Then $\langle ab \rangle = ab - pc$. So another way to express μ is

$$\mu = \#\left\{(b, c) \in \mathbb{Z}^2 \;\middle|\; 0 < b < \frac{p}{2}, -\frac{p}{2} < ab - pc < 0\right\}.$$

Theorem 2.7 (Law of Quadratic Reciprocity)**.** Let p, q be distinct odd primes. Then

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

Equivalently,

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

Proof. We know $\left(\frac{q}{p}\right) = (-1)^\mu$,

$$\mu = \#\left\{(b, c) \in \mathbb{Z}^2 \;\middle|\; 0 < b < \frac{p}{2}, -\frac{p}{2} < qb - pc < 0\right\}.$$

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

$$\begin{aligned} \nu &= \#\left\{(b, c) \in \mathbb{Z}^2 \;\middle|\; 0 < b < \frac{q}{2}, -\frac{q}{2} < pb - qc < 0\right\} \\ &= \#\left\{(b, c) \in \mathbb{Z}^2 \;\middle|\; 0 < c < \frac{q}{2}, 0 < qb - pc < \frac{q}{2}\right\} \end{aligned}$$

Define

$$A = \left\{ (b,c) \in \mathbb{Z}^2 \;\middle|\; 0 < b < \frac{p}{2}, -\frac{p}{2} < qb - pc < 0 \right\}$$
$$B = \left\{ (b,c) \in \mathbb{Z}^2 \;\middle|\; 0 < c < \frac{q}{2}, 0 < qb - pc < \frac{q}{2} \right\}$$

(so $\mu = \#A$, $\nu = \#B$).

Claim: A, B are disjoint subsets of

$$S = \left\{ (b,c) \in \mathbb{Z}^2 \;\middle|\; 0 < b < \frac{p}{2}, 0 < c < \frac{q}{2} \right\}.$$

Why? $A \subset S$. We need to show $(b,c) \in A$ implies $0 < c < \frac{q}{2}$. We have $pc > qb > 0 \implies c > 0$, and

$$pc < qb + \frac{p}{2} < \frac{qp}{2} + \frac{p}{2} \implies c < \frac{q+1}{2} \implies c < \frac{q}{2}$$

(since $c \in \mathbb{Z}$, q odd). Similarly, $B \subset S$. A, B are disjoint because $qb - pc < 0$ in A, $qb - pc > 0$ in B.

We have $\#S = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$, so

$$\begin{aligned} \text{desired result} &\iff (-1)^{\#A+\#B} = (-1)^{\#S} \\ &\iff \#(A \sqcup B) \equiv \#S \pmod 2 \\ &\iff \#(S \setminus (A \cup B)) \text{ is even} \end{aligned}$$

Note

$$S \setminus (A \cup B) = \left\{ (b,c) \in S \;\middle|\; qb - pc < -\frac{p}{2} \right\} \sqcup \left\{ (b,c) \in S \;\middle|\; qb - pc > \frac{q}{2} \right\} =: X \sqcup Y$$

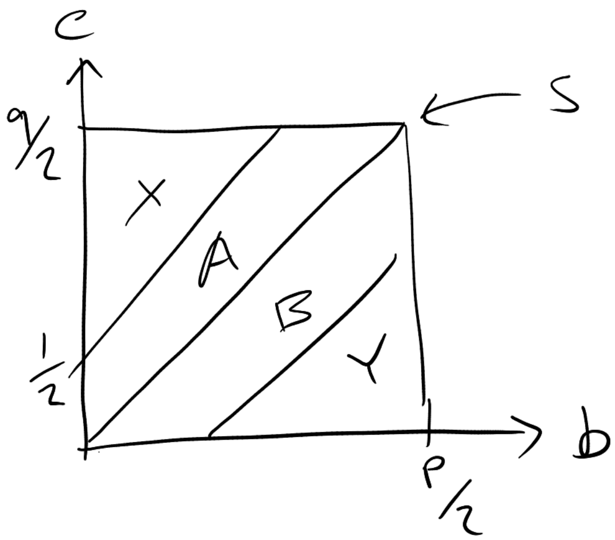
We'll show $\#X = \#Y$.

Consider the map $\theta : S \to S$, $\theta(b,c) = \left(\frac{p+1}{2} - b, \frac{q+1}{2} - c\right)$. We have $\theta^2 = \mathrm{id}$, hence θ is surjective, hence bijective since S is finite. To show $\#X = \#Y$, it's enough to show $\theta(X) = Y$. If $(b,c) \in S$, then $(b,c) \in X \iff qb - pc < -\frac{p}{2}$.

$$\begin{aligned} \theta(b,c) \in Y &\iff q\left(\frac{p+1}{2} - b\right) - p\left(\frac{q+1}{2} - c\right) > \frac{q}{2} \\ &\iff \frac{q}{2} - qb - \frac{p}{2} + pc > \frac{q}{2} \\ &\iff pc - qb > \frac{p}{2} \\ &\iff (b,c) \in X \end{aligned}$$

□

Picture of proof:



$$A = \left\{ (b,c) \in S \;\middle|\; -\frac{p}{2} < qb - pc < 0 \right\}$$

$$-\frac{p}{2} = qb - pc \iff c = \frac{q}{p}b + \frac{1}{2}$$

Example. Let $p \geq 5$. We determine $\left(\frac{3}{p}\right)$ using Law of Quadratic Reciprocity. We have

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

$\left(\frac{p}{3}\right)$ only depends on p modulo 3. In particular

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

We find

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

Example. Question: Does the equation $X^2 = 19$ have a solution in $\mathbb{Z}/73\mathbb{Z}$? 73 is prime, so this happens if and only if $\left(\frac{19}{73}\right) = 1$. 19 is also prime, so this equals

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

as 16 is a square number (and using $73 = 3 \times 19 + 6$).

Example.

$$\begin{aligned}
\left(\frac{34}{97}\right) &= \left(\frac{2 \times 2}{97}\right) \\
&= \left(\frac{2}{97}\right)\left(\frac{2}{97}\right) \\
&= \left(\frac{17}{97}\right) \\
&= \left(\frac{97}{17}\right) \\
&= \left(\frac{12}{17}\right) \\
&= \left(\frac{3}{17}\right)\left(\frac{4}{17}\right) \\
&= \left(\frac{3}{17}\right) \\
&= -1
\end{aligned}$$

Example.

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

To compute Legendre symbols without factorising, we can use the Jacobi symbol.

Definition 2.8 (Jacobi Symbol)**.** Let $N \in \mathbb{N}$ be odd with prime factorisation $N = p_1 \cdots p_k$, noting that the p_i's need not be distinct. Then for $a \in \mathbb{Z}$, we define the *Jacobi symbol* as

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

where the right hand side is a product of Legendre symbols.

Start of lecture 8

Remark. If $(a, N) > 1$, then $\left(\frac{a}{N}\right) = 0$, as if $p \mid (a, N)$ then $\left(\frac{a}{p}\right) = 0$. If N is prime, then $\left(\frac{a}{N}\right)$ is well-defined (because Jacobi symbol equals the Legendre symbol).

Example.

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

Warning. The Jacobi symbol does not tell you whether a is a square modulo N (except when N is prime). For example, 2 is not a square modulo 15 (since it isn't a square modulo 3), but as seen in the previous example, $\left(\frac{2}{15}\right) = 1$.

If $N = pq$, where p and q are distinct odd primes, then $a \bmod pq$ is a square if and only if $a \bmod p$ is a square and $a \bmod q$ is a square, which happens if and only if $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$.

But we have $\left(\frac{a}{N}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = 1$, which happens if and only if either $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$ *or* $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$.

In general, to decide is $a \bmod N$ is a square, we need to factorise N.

Lemma 2.9 (Jacobi formulae)**.** Let $M, N \in \mathbb{N}$ be odd, $a, b \in \mathbb{Z}$. Then:

(1) If $a \equiv b \pmod N$, then $\left(\frac{a}{N}\right) = \left(\frac{b}{N}\right)$.

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

(3) $\left(\frac{a}{MN}\right) = \left(\frac{a}{M}\right)\left(\frac{a}{N}\right)$.

Proof.

(1) If $N = p_1 \cdots p_r$, then

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

If $a \equiv b \pmod{N}$, then $a \equiv b \pmod{p}$ $\forall p \mid N$. If $p \mid N$ is prime, then $\left(\frac{a}{p}\right)$ only depends on $a \bmod p$. So indeed

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

if $a \equiv b \pmod{N}$.

(2)

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

(3) If $N = p_1 \cdots p_r$, $M = q_1 \cdots q_s$, then $NM = p_1 \cdots p_r q_1 \cdots q_s$, so

$$\left(\frac{a}{MN}\right) = \left(\prod_{i=1}^{r} \left(\frac{a}{p_i}\right)\right)\left(\prod_{j=1}^{s} \left(\frac{a}{q_j}\right)\right) = \left(\frac{a}{M}\right)\left(\frac{a}{N}\right)$$ □

Proposition 2.10. If $N \in \mathbb{N}$ is odd, then

$$\left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}} = \begin{cases} 1 & N \equiv \quad \pmod{4} \\ -1 & N \equiv 3 \pmod{4} \end{cases}$$

$$\left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}} = \begin{cases} 1 & N \equiv \pm 1 \pmod{8} \\ -1 & N \equiv \pm 5 \pmod{8} \end{cases}$$

Proof. If $N = p_1 \cdots p_r$, then

$$\left(\frac{-1}{N}\right) = \prod_{i=1}^{r} \left(\frac{-1}{p_i}\right) = \prod_{i=1}^{r} (-1)^{\frac{p_i-1}{2}}$$

We need to show that if $a, b \in \mathbb{Z}$ are odd, then $(-1)^{\frac{a-1}{2}}(-1)^{\frac{b-1}{2}} = (-1)^{\frac{ab-1}{2}}$. We have:

$$\begin{aligned}
2 \mid a-1, 2 \mid b-1 &\implies (a-1)(b-1) \equiv 0 \pmod 4 \\
&\implies ab - a - b + 1 \equiv 0 \pmod 4 \\
&\equiv ab - 1 \equiv (a-1) + (b-1) \pmod 4 \\
&\implies \frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2 \\
&\implies (-1)^{\frac{ab-1}{2}} = (-1)^{\frac{a-1}{2}} \cdot (-1)^{\frac{b-1}{2}}
\end{aligned}$$

Similarly, we compute

$$\left(\frac{2}{N}\right) = \prod_{i=1}^{r} \left(\frac{2}{p_i}\right) = \prod_{i=1}^{r} (-1)^{\frac{p_i^2-1}{8}}$$

We need to check that if $a, b \in \mathbb{Z}$ are odd, then $(-1)^{\frac{a^2-1}{8}} \cdot (-1)^{\frac{b^2-1}{8}} = (-1)^{\frac{(ab)^2-1}{8}}$. We have

$$\begin{aligned}
a^2 \equiv 1 \pmod 4, b^2 \equiv 1 \pmod 4 &\implies (a^2-1)(b^2-1) \equiv 0 \pmod{16} \\
&\implies a^2b^2 - 1 \equiv (a^2-1) + (b^2-1) \pmod{16} \\
&\implies \frac{(ab)^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod 2 \qquad \square
\end{aligned}$$

Theorem 2.11 (Quadratic Reciprocity for Jacobi symbols)**.** Let $M, N \in \mathbb{N}$ be odd. Then

$$\left(\frac{M}{N}\right) = \left(\frac{N}{M}\right) \cdot (-1)^{\left(\frac{M-1}{2}\right)\left(\frac{N-1}{2}\right)}$$

If $(M, N) = 1$, then

$$\left(\frac{M}{N}\right)\left(\frac{N}{M}\right) = (-1)^{\left(\frac{M-1}{2}\right)\left(\frac{N-1}{2}\right)}.$$

Proof. Factorise $M = q_1 \cdots q_s$, $N = p_1 \cdots p_r$. Let $k = \#\{j \mid q_j \equiv 3 \pmod 4\}$, $l = \#\{i \mid p_i \equiv 3 \pmod 4\}$. We can assume M and N are coprime (since if they have a common factor, the Jacobi symbols will both be zero). Then

$$\begin{aligned}\left(\frac{M}{N}\right) &= \prod_{i=1}^{r}\left(\frac{M}{p_i}\right)\\ &= \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)\\ &= (-1)^{kl}\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)\\ &= (-1)^{kl}\left(\frac{N}{M}\right)\end{aligned}$$

We need to show $(-1)^{kl} = (-1)^{\left(\frac{M-1}{2}\right)\left(\frac{N-1}{2}\right)}$. We know $M \equiv 3 \pmod 4$ if and only if k is odd. Similarly, $N \equiv 3 \pmod 4$ if and only if l is odd. So:

$$\begin{aligned}\text{RHS is } -1 &\iff M, N \equiv 3 \pmod 4\\ &\iff \text{both } k \text{ and } l \text{ are odd}\\ &\iff kl \text{ is odd}\\ &\iff (-1)^{kl} = -1\end{aligned}$$

□

Example. We can use the Jacobi symbol to compute Legendre symbols without factoring. For example:

$$\left(\frac{33}{73}\right) = \left(\frac{73}{33}\right) = \left(\frac{7}{33}\right) = \left(\frac{33}{7}\right) = \left(\frac{5}{7}\right)\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Another example (using the above, noting that we first factor out the 2 because Quadratic Reciprocity for Jacobi symbols requires both numbers to be odd):

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

3 Binary Quadratic Forms

Theorem 3.1 (Fermat-Euler)**.** If $N \in \mathbb{N}$, then we can write $N = x^2 + y^2$, $x, y \in \mathbb{Z}$ if and only if for every prime number p such that $p \mid N$ and $p \equiv 3 \pmod 4$, then p divides N an even number of times.

In particular, if q is an odd prime, then $Q = x^2 + y^2 \iff q \equiv \pmod 4$.

In GRM, this is proved using unique factorisation in $\mathbb{Z}[i]$.

Here, we will develop a general theory that applies to $x^2 + y^2$ (an example of a BQF) and also to $x^2 + 2y^2$, $x^2 + 3y^2$, ...

Start of

lecture 9

Motivating question: Which integers can be expressed as $x^2 + y^2$, $x^2 + 2y^2$?

Definition 3.2 (BQF)**.** A *binary quadratic form* (BQF) is a polynomial $f(x, y) = ax^2 + bxy + cy^2$ where $a, b, c \in \mathbb{Z}$.

If $N \in \mathbb{Z}$, we say f *represents* N if $\exists m, n \in \mathbb{Z}$ such that $f(m, n) = N$.

Notation. We will sometimes identify f with the tuple (a, b, c), or with the matrix

$$\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$$

This is because we can write

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

Example.

$$f(x, y) = x^2 + y^2 \leftrightarrow (1, 0, 1) \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$g(x, y) = 4x^2 + 12xy + 10y^2 \leftrightarrow (4, 12, 0) \leftrightarrow \begin{pmatrix} 4 & 6 \\ 6 & 10 \end{pmatrix}$$

Key idea: study the effect on binary quadratic forms of changes of variable.

Using the functions as in the example above, we have

$$g(x,y) = (2x+5y)^2 + y^2 = f(2x+3y, y).$$

However, f and g do not represent the same sets of integers (as e.g. g can only represent event integers wheres f represents 1).

Definition 3.3 (Unimodular change of variables)**.**

(1) A unimodular change of variables is one of the form $X = \alpha x + \gamma y$, $Y = \beta x + \delta y$, where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ with $\alpha\delta - \beta\gamma = 1$.

(2) We say that two BQFs $f(x,y)$, $g(x,y)$ are *equivalent* if there exists a unimdular change of variables such that $g(x,y) = f(X,Y) = f(\alpha x + \gamma y, \beta x + \delta y)$. Equivalently, if there exists $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $g(x,y) = f((x,y)A)$.

Remark. $X = 2x+3y$, $Y = y$ is *not* aunimodular change of variables, since

$$\det \begin{pmatrix} 2 & 0 \\ 3 & 1 \end{pmatrix} = 2 \neq 1.$$

Equivalence of BQFs is an equivalence relation. This is because $\mathrm{SL}_2(\mathbb{Z})$ is a group (so for example, symmetry comes from the fact that inverses exist).

$\mathrm{SL}_2(\mathbb{Z})$ acts on the set of BQFs via $(A \cdot f)(x,y) = f((x,y)A)$. Two forms f and g are equivalent if and only if they're in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit.

If f, g are equivalent binary quadratic form, then they represent the same sets of integers. This is because by symmetry, we need to show that if $g(x,y) = f(\alpha x + \gamma y, \beta x + \delta y)$, and g represents N, then f also represents N.

Definition 3.4 (BQF discriminant)**.** The *discriminant* of a binary quadratic form $f = (a,b,c)$ is

$$\operatorname{disc} f = b^2 - 4ac.$$

Lemma 3.5. equivalent forms have the same discriminant.

Proof. We need to check that $\operatorname{disc} f = \operatorname{disc}(A \cdot f)$ if $f = (a,b,c)$, $A \in \mathrm{SL}_2(\mathbb{Z})$. If $f = (a,b,c)$, then

$$f \leftrightarrow \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$$

which has determinant $ac - \frac{b^2}{4} = -\frac{1}{4}\operatorname{disc} f$. We have

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

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

so

$$A \cdot f \leftrightarrow A\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}A^\top$$

Therefore

$$\det\left(A\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}A^\top\right) = \det(A)\det\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\det(A) = \det\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \qquad \square$$

Remark. Converse does not hold: $x^2 + 6y^2$, $2x^2 + 3y^2$ have the same discriminant (-24), but not equivalent as they do not represent the same integers (the first form represents 1, whereas the second does not).

Lemma 3.6. Let $d \in \mathbb{Z}$. Then there exist BQFs of discriminant d if and only if $d \equiv 0$ or $1 \pmod 4$.

Proof. If $d = \operatorname{disc} f$, $f = (a,b,c)$, then $d = b^2 - 4ac \equiv b^2 \pmod 4$. So must be 0 or 1 modulo 4.

If $d \equiv 0 \pmod 4$, then $x^2 - \frac{d}{4}y^2$ is a BQF of discriminant d.

If $d \equiv 1 \pmod 4$, then $x^2 + xy + \frac{1-d}{4}y^2$ is a BQF of discriminant d. $\square$

Definition 3.7. Let $f(x_1, \ldots, x_n) = \sum_{i \leq j} a_{ij}x_ix_j$ be a (real) quadratic form, $a_{ij} \in \mathbb{R}$. We say f is:

- *positive definite* if $\forall \mathbf{v} \in \mathbb{R}^n - \{0\}$, $f(\mathbf{v}) > 0$.
- *negative definite* if $\forall \mathbf{v} \in \mathbb{R}^n - \{0\}$, $f(\mathbf{v}) < 0$.
- *indefinite* if $\exists \mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ such that $f(\mathbf{v}) > 0$, $f(\mathbf{w}) < 0$.

Proposition 3.8. Let $f(x,y) = ax^2 + bxy + cy^2$ be a BQF of discriminant $d \in \mathbb{Z}$. Then:

(1) If $d < 0$, $a > 0$, then f is positive definite. If $d < 0$, $a > 0$, f is negative definite.

(2) If $d > 0$, f is indefinite.

(3) If $d = 0$, then $\exists l, m, n \in \mathbb{Z}$ such that $f(x,y) = l(mx + ny)^2$.

Proof.

(1) If $d < 0$, then $a \neq 0$ and

$$4f(x,y) = 4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 + (4ac - b^2)y^2 = (2ax + by)^2 - dy^2.$$

So $4af(x,y)$ is positive definite.

(2) If $d > 0$, then we can factor $f(x,1) = a(x - \alpha)(x - \beta)$, $\alpha, \beta \in \mathbb{R}$, provided $a \neq 0$, using the quadratic formula. Since $d \neq 0$, $\alpha \neq \beta$, so we can assume $\alpha < \beta$. If $v, w \in \mathbb{R}$, $v < \alpha$, $w \in (\alpha, \beta)$, then $f(v,1)$ and $f(w,1)$ are non-zero real numbers of opposite signs. So f is indefinite. If $a = c = 0$, then $f(x,y) = bxy$ with $b \neq 0$, clearly indefinite.

(3) If $d = 0$, then $b^2 = 4ac$. Write $a = a_1a_2^2$, $a_1, a_2 \in \mathbb{Z}$ squarefree. Then $b^2 = 4a_1a_2^2c$, so a_1c is a square, so $a_1 \mid c$, $c = a_1z^2$, $z \in ZZ$. Then $f(x,y) = ax^2 + bxy + cy^2 = a_1a_2^2x^2 + bxy + cy^2 = a_1\left(a_2x + \frac{b}{2a_1a_2}y\right)^2$.

□

Start of lecture 10

Remark. (This remark is unrelated to the current content). Given that we know that a primitive root exists modulo any prime, one question we might ask is :“Can a be a primitive root for all sufficiently large primes p?”

The answer is no. One can prove this using the Jacobi symbol and Dirichlet's Theorem on primes in arithmetic progressions.

We know:

- equivalent forms represent the same integers ($N = f(m,n)$, $m, n \in \mathbb{Z}$).

- equivalent forms have the same discriminant.
- Equivalence is an equivalence relation.

We said that a BQF $f(x,y)$ is positive definite if $\forall \mathbf{v} \in \mathbb{R}^2 - 0,\ f(\mathbf{v}) > 0$. We showed that f is positive definite $\iff$ $\operatorname{disc} f < 0,\ a > 0,\ \iff$ $\operatorname{disc} f < 0,\ c > 0$.

We will now study equivalence classes of PDBQFs (positive definite binary quadratic forms) of fixed discriminant $d \in \mathbb{Z}$, $d \equiv 0, 1 \pmod 4$, $d < 0$. The set of classes is always non-empty since

$$x^2 + \frac{d}{4}y^2 \qquad \text{or} \qquad x^2 + y + \frac{(1-d)}{4}y^2$$

is a PDBQF of discriminant d.

Question: If we are given a PDBQF (a, b, c), when can we find an equivalent one with smaller coefficients?

Example. $f(x,y) = 10x^2 + 34xy + 29y^2 = (10, 34, 29)$. We try to decrease the coefficients by acting by the unimodular changes of variables

$$T_\pm = \begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix} \qquad \text{and} \qquad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Fact: $S_1, T_\pm$ generate $\mathrm{SL}_2(\mathbb{Z})$, so any unimdular change of variables is a composite of these.

If $g(x,y) = ax^2 + bxy + cy^2$, then for $\lambda = \pm 1$,

$$\begin{aligned}(T_\lambda g)(x,y) &= g((x,y)T_\lambda) \\ &= g(x + \lambda y, y) \\ &= a(x+\lambda y)^2 + b(x+\lambda y)y + cy^2 \\ &= ax^2 + (b + 2a\lambda)xy + (c + b\lambda + a\lambda^2)y^2\end{aligned}$$

So $T_\pm : (a,b,c) \mapsto (a, b \pm 2a, c \pm b + a)$. So we can make unimdular change of variables for f as follows:

$$(10, 34, 29) \underset{T_-}{\longrightarrow} (10, 14, 5) \underset{T_-}{\longrightarrow} (10, -6, 1).$$

We have

$$(S \cdot g)(x,y) = g\left((x,y)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = g(-y, x) = cx^2 - bxy + ay^2.$$

If $a > c$, we can act by S to reduce the size of a, just as when $|b| > 2a$ we could act by one of T_+, T_- to reduce the size of b.

$$(10, -6, 1) \underset{S}{\longrightarrow} (1, 6, 10) \underset{T_-}{\longrightarrow} (1, 4, 5) \underset{T_-}{\longrightarrow} (1, 2, 2) \underset{T_-}{\longrightarrow} (1, 0, 1).$$

We've proved that $f(x,y) = 10x^2 + 34xy + 29y^2$ is equivalent to $x^2 + y^2$.

Definition 3.9 (Reduced PDBQF)**.** We say a PDBQF (a,b,c) is *reduced* if $-a < b \le a \le c$ and if $a = c$, then $b \ge 0$.

Example. $10x^2 + 34xy + 29y^2$ is not reduced. $x^2 + y^2$ is reduced.

In general, if (a,b,c) is reduced, then $c \ge a \ge |b| \ge 0$.

Proposition 3.10. Any PDBQF is equivalent to a reduced one.

Proof. Starting with (a, b, c) we act as follows. If $a > c$, then act by S to replace (a, b, c) by $(c, -b, a)$. This decreases a and doesn't change $|b|$. If $a \leq c$, but $|b| > a$, then act by one of $T_\pm : (a, b, c) \to (a, b \pm 2a, c \pm b + a)$ to decrease $|b|$ and leave a the same.

Repeat these steps until $a \leq c$ and $|b| \leq a$. The process must terminate as $a + |b|$ is a positive integer, but decreases by at least 1 each time we act by ± 1.

The form (a, b, c) is then reduced except possibly if $c > a$ and $b = -a$ or if $a = c$ and $b < 0$. If $c > a$, $b = -a$, then $f = (a, -a, c)$, $T_+ f = (a, a, c)$ is reduced. If $c = a$, $b < 0$, then $f = (a, b, a)$, $Sf = (a, -b, a)$ is reduced. □

Lemma 3.11. If (a, b, c) is a reduced PDBQF then $|b| \leq a \leq \sqrt{\frac{|d|}{3}}$, where $d = b^2 - 4ac$ and $b \equiv d \pmod 2$.

Proof. $b^2 \equiv d \pmod 4 \implies b \equiv d \pmod 2$. We have $c \geq a \geq |b| \geq 0$, $-d = 4ac - b^2 \geq 4ac - ac = 3ac \geq 3a^2$

$$\implies a \leq \sqrt{\frac{|d|}{3}}$$ □

Example. Let's enumerate all reduced forms of discriminant -4. If (a, b, c) is reduced, $b^2 - 4ac = 4$, then $c \geq a \geq |b| \geq 0$, $b \equiv 0 \pmod 2$, $a \leq \sqrt{\frac{4}{3}}$ so $a = 1$. Since b is even, $|b| \leq 1$, we must have $b = 0$. Since $b^2 - 4ac = -4$, this fixes $c = 1$. So $x^2 + y^2$ is the only reduced of discriminant -4, so any PDBQF of discriminant -4 is equivalent to $x^2 + y^2$.

Corollary 3.12. If p is an odd prime, then p is represent $x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$.

Proof.

$\Rightarrow$ Easy.

$\Leftarrow$ We know $p \equiv 1 \pmod 4$ implies $\left(\frac{-1}{p}\right) = 1$, so there exists $n \in \mathbb{Z}$ such that $n^2 \equiv -1 \pmod p$. So $\exists n, k \in \mathbb{Z}$ such that $n^2 = -1 + pk$. Then $-4 = 4n^2 - 4pk = \mathrm{disc}(px^2 +$

$2nxy + ky^2$). So $f(x,y) = px^2 + 2nxy + ky^2$ is a PDBQF of discriminant -4, which represents p, as $f(1,0) = p$. f is equivalent to the reduced form $x^2 + y^2$. Equivalent forms represent the same integers, so $x^2 + y^2$ represents p. □

Start of lecture 11

Corollary 3.13. Let $d \in \mathbb{Z}$, $d < 0$, $d \equiv 0$ or $1 \pmod 4$. Then the number of equivalence classes of PDBQF of discriminant d is finite.

Proof. Every equivalence class contains a reduced form. Therefore it is enough to show that there are finitely many reduced (a,b,c) of disc d. If (a,b,c) is reduced, then $|b| \le a \le \sqrt{\frac{|d|}{3}}$, so there are finitely many choices for a and b. But we also know $c = \frac{b^2-d}{4a}$, so a and b determine c. □

Definition 3.14. Let $f = (a,b,c)$ be a binary quadratic form, $N \in \mathbb{Z}$. We say N is *properly represented* by f if $\exists m, n \in \mathbb{Z}$ with $f(m,n) = N$ with $\gcd(m,n) = 1$.

Note. If f, g are equivalent, then they properly represent the same integers. Why? By symmetry, enough to show that if f properly represents N, then so does g. Suppose $f(m,n) = N$, $\gcd(m,n) = 1$. Let $f(x,y) = g((x,y)A)$,

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

Then $f(m,n) = N = g((m,n)A) = g(\alpha m + \gamma n, \beta m + \delta n)$. We need to check $\gcd(\alpha m + \gamma n, \beta m + \delta n) = 1$.

We have $\gcd(m,n) \mid \alpha m + \gamma n, \beta m + \delta n$, so $\gcd(m,n) \mid \gcd(\alpha m + \gamma n, \beta m + \delta n)$. Since $(\alpha m + \gamma n, \beta m + \delta n) = (m,n)A$, we have $(m,n) = (\alpha m + \gamma n, \beta m + \delta n)A^{-1}$, $A^{-1} \in \mathrm{SL}_2(\mathbb{Z})$. So the same argument gives $\gcd(\alpha m + \gamma n, \beta m + \delta n) \mid \gcd(m,n)$, so equality holds. So g properly represents N.

Lemma 3.15. Let $f = (a, b, c)$ be a reduced PDBQF. Then

(1) $a \le c \le a + c - |b|$.

(2) $f(1, 0) = a$, $f(0, 1) = c$, $\exists \varepsilon \in \{\pm 1\}$ with $f(1, \varepsilon) = a + c - |b|$.

(3) If $m, n \in \mathbb{Z}, \gcd(m, n) = 1$, and $(m, n) \neq \pm(1, 0)$ or $\pm(0, 1)$ then $f(m, n) \ge a + c - |b|$.

Informally: the smallest 3 properly represented values of f are a, c, $a + c - |b|$.

Proof.

(1) Since f is reduced, $c \ge a \ge |b| \ge 0$. So $a - |b| \ge 0$, $c + a - |b| \ge c$.

(2) $f(x, y) = ax^2 + bxy + cy^2 \implies f(1, 0) = a$, $f(0, 1) = c$, $f(1, \varepsilon) = a + \varepsilon + c$, $\varepsilon \in \{\pm 1\}$. Choose ε so that $\varepsilon b = -|b|$. Then $f(1, \varepsilon) = a + c - |b|$.

(3) If $m, n \in \mathbb{Z}$, $\gcd(m, n) = 1$, and $(m, n) \neq \pm(1, 0)$ or $\pm(0, 1)$, then m, n are both non-zero. First assume $|m| \ge |n| \ge 1$. Then $f(m, n) = am^2 + bmn + cn^2 \ge am^2 - |b|m^2 + cn^2 \ge (a - |b|)m^2 + cn^2$. Since f is reduced, $a - |b| \ge 0$. Then since $m^2, n^2 \ge 1$, $f(m, n) \ge a + c - |b|$. Next assume $|n| \ge |m| \ge 1$. Then

$$f(m, n) = am^2 + bmn + cn^2 \ge am^2 - |b|n^2 + cn^2 \ge am^2 + (c - |b|)n^2 \ge a + c - |b| \quad \square$$

Theorem 3.16. Every PDBQF is equivalent to a unique reduced form.

Proof. Every PDBQF is equivalent to some reduced form, so it's enough to show that if $f = (a, b, c)$, $g = (a', b', c')$ are equivalent reduced forms, then they're equal.

We know that equivalent forms properly represent the same values, the same number of times. We know that the 3 smallest values represented by f are $a \le c \le a + c - |b|$, and the ones for g are $a' \le c' \le a' + c' - |b'|$. So $a = a'$, $c = c'$, $a + c - |b| = a' + c' - |b'|$, so $|b| = |b'|$, $b' = \pm b$. Assume for contradiction that $b \neq b'$, then without loss of generality we can assume $b > 0$. So $f = (a, b, c)$, $g = (a, -b, c)$. Recall to say f is reduced means $c \ge a \ge |b|$, and if $c = a$ or $a = |b|$, then $b \ge 0$.

We're assuming $b > 0$, and $g = (a, -b, c)$ is also reduced. Therefore we must have $c > a$, $a > b$, so $a < c < a + c - b$. Suppose $f(x, y) = g((x, y)A)$, $A \in \mathrm{SL}_2(\mathbb{Z})$,

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

Then $a = f(1,0) = g((1,0)A) = g(\alpha, \beta)$ and $c = f(0,1) = g(\gamma, \delta)$. We have $\gcd(\alpha, \beta) = 1$, $\gcd(\gamma, \delta) = 1$. By Lemma 3.15(3), we know that if $m, n \in \mathbb{Z}$, $\gcd(m,n) = 1$, $(m,n) \neq \pm(1,0)$ or $\pm(0,1)$, then $g(m,n) \geq a + c - |b| > c$. The only possibilities are $(\alpha, \beta) = \pm(1,0)$, $\gamma, \delta) = \pm(0,1)$. Hence

$$A = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$$

Since $\det(A) = 1$, we must have both signs the same, so $A = \pm I_2$. Hence $g((x,y)A) = g(\pm(x,y)) = g(x,y)$ (since g is homogeneous of degree 2). But $f(x,y) = g((x,y)A) = f(x,y)$, so $g(x,y) = f(x,y)$, contradicting our assumption that they were non-equal. □

Definition 3.17. Let $d \in \mathbb{Z}$, $d < 0$, $d \equiv 0, 1 \pmod 4$. Then we write

$$\begin{aligned} h(d) &= \#\{\text{equivalence classes of PDBQF of discriminant } d\} \\ &= \#\{\text{reduced PDBQFs of discriminant } d\} \end{aligned}$$

"Class number of d"

Example. $h(-4) = 1$. Let's compute $h(-24)$ by enumerating reduced forms. TODO???

Start of lecture 12

Lemma 3.18. Let $f(x,y)$ be a PDBQF, $N \in \mathbb{N}$. Then f properly represents N if and only if f is equivalent to a form $g = (a,b,c)$ where $a = N$.

Proof.

$\Leftarrow$ equivalent forms properly represent the same integers. Since $g(1,0) = N$, f properly represents N.

$\Rightarrow$ Suppose $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $g(x,y) = f((x,y)A) = (a,b,c)$. Then $g(1,0) = a$. By assumption, $\exists m, n \in \mathbb{Z}$ with $\gcd(m,n) = 1$, $f(m,n) = N$. $a = g(1,0) = f((1,0)A)$. If we can choose A so that $(1,0) = (m,n)$, then we will have $a = g(1,0) = f(m,n) = N$. Since $\gcd(m,n) = 1$, $\exists r, s \in \mathbb{Z}$ such that $rm + sn = 1$. If

$$A = \begin{pmatrix} m & n \\ -s & r \end{pmatrix},$$

then $\det(A) = 1$, so $A \in \mathrm{SL}_2(\mathbb{Z})$, and $(1,0)A = (m,n)$. □

Theorem 3.19. Let $d \in \mathbb{Z}$, $d < 0$, $d \equiv 0$ or $1 \pmod 4$. Let $N \in \mathbb{N}$. Then the following are equivalent:

(i) N is properly represent by some PDBQF of discriminant d.

(ii) The congruence $X^2 \equiv d \pmod{4N}$ has a solution.

Proof.

(1) $\implies$ (2) By Lemma 3.18, (1) holds if and only if $\exists$ PDBQF (N, b, c) of discriminant d. Then $d = b^2 - 4Nc$ so b is a solution to $X^2 \equiv d \pmod{4N}$.

(2) $\implies$ (1) Suppose there is a solution $b \in \mathbb{Z}$. Then $b^2 \equiv d \pmod{4N}$, so there exists $c \in \mathbb{Z}$ such that $b^2 = d + 4Nc$. Then $f(x, y) = (N, b, c)$ has discriminant $b^2 - 4Nc = d$. So f is a PDBQF of discriminant d which properly represents N.

□

Example. $f(x,y) = x^2 + xy + 2y^2$, a PDBQF of discriminant $d = -7$. Which integers are represent by f?

First decide which $N \in \mathbb{N}$ are properly represent by $f(x,y)$. Claim: $h(-7) = 1$. If (a,b,c) is a reduced form of discriminant -7, then $|b| \le a \le \sqrt{7/3} < 2$ so $|b| \le a \le 1$. Also, b is odd. So $a = 1$, $b = 1$, $c = 2$ and $(a,b,c) = (1,1,2)$. By Theorem 3.19, N is properly represent by some form of discriminant -7 if and only if $X^2 \equiv -7 \pmod{4N}$ has a solution. Hence N is properly represent by $f(x,y)$ if and only if $X^2 \equiv -7 \pmod{4N}$ has a solution. Let's analyse the congruence condition $X^2 \equiv -7 \pmod{4N}$ first when $N = p$ prime. If $N = p = 2$: want $X^2 \equiv -7 \equiv 1 \pmod 8$ to have a solution (which it does).

If p is odd: by Chinese Remainder Theorem, want the two congruences

$$\begin{cases} X^2 \equiv -7 \equiv 1 \pmod 4 \\ X^2 \equiv -7 \equiv \pmod p \end{cases}$$

to both be solvable. If $p = 7$, this is solvable. If $p \neq 2, 7$, this is solvable

$$\iff \left(\frac{-7}{p}\right) = 1 \overset{\text{QR}}{\iff} \left(\frac{p}{7}\right) = 1 \iff p \equiv 1, 2, \text{ or } 4 \pmod 7.$$

So a prime number p is properly represented by $f(x,y) \iff p \equiv 0, 1, 2$ or $4 \pmod 7$. Now suppose N is not necessarily prime, and write $N = \prod_p p^{e_p}$, p prime, $e_p \ge 0$. Then N is properly represented by $f \iff X^2 \equiv -7 \pmod{4N}$ has a solution

$$\overset{\text{Chinese Remainder Theorem}}{\iff} \begin{cases} X^2 \equiv -7 \pmod{2^{e_2+2}} \\ X^2 \equiv -7 \pmod{p^{e_p}} & p \text{ odd} \end{cases}$$

are all solvable.

Lemma 3.20. Let $a \in \mathbb{Z}$. Then

(1) If p is an odd prime and $\left(\frac{a}{p}\right) = 1$, then the congruence $X^2 \equiv a \pmod{p^k}$ is solvable $\forall k \ge 1$.

(2) If $a \equiv 1 \pmod 8$, then $X^2 \equiv a \pmod{2^k}$ is solvable $\forall k \ge 1$.

Proof.

(1) Use induction on $k \ge 1$, $k = 1$ holding by assumption. Suppose $\exists x, y \in \mathbb{Z}$ such that

$x^2 = a + yp^k$. Consider for $z \in \mathbb{Z}$

$$(x + p^k z)^2 = x^2 + 2p^k xz + p^{2k} z^2 \equiv a + p^k(y + 2xz) \pmod{p^{k+1}}$$

This is congruend to $a \pmod{p^{k+1}} \iff y \equiv -2xz \pmod{p}$. Since p is odd, $p \nmid a \implies p \nmid x$, so $(2x, p) = 1$, so we can find $z \in \mathbb{Z}$ such that $-2xz \equiv y \pmod{p}$.

(2) We show $X^2 \equiv a \pmod{2^k}$ has a solution for all $k \ge 3$ by induction on $k \ge 3$. $k = 3$ holds by assumption. Suppose $\exists x, y \in \mathbb{Z}$ such that $x^2 = a + 2^k y$, $k \ge 3$. If y is even, then $x^2 \equiv a \pmod{2^{k+1}}$. So assume y is odd. Then

$$(x + 2^{k-1})^2 = x^2 + 2^k x + 2^{2k-2} = a + a^k(x + y) + 2^{2k-2}$$

so $x + y$ is even (since both x and y are odd). So

$$(x + 2^{k-1})^2 \equiv a + 2^{2k-2} \pmod{2^{k+1}}$$

This is congruent to $a \pmod{2^{k+1}}$ if and only if $2k - 2 \ge k + 1$, which is true if and only if $k \ge 3$. □

Conclusion: $N \in NN$ is properly represented by $x^2 + xy + 2y^2$ if and only if the congruences $X^2 \equiv -7 \pmod{2^{e_2+2}}$, $X^2 \equiv -7 \pmod{p^{e_p}}$ (p odd, $e_p \ge 1$) are all solvable. The first is always solvable, so this is true:

$$\begin{aligned} &\iff \text{if } p \mid N,\ p \neq 2, 7, \text{ then } p \equiv 1, 2 \text{ or } 4 \pmod{7} \text{ and} \\ &\ \text{if } 7 \mid N, \text{ then } X^2 \equiv -7 \pmod{7^{e_7}} \text{ has a solution} \\ &\iff \text{if } p \mid N,\ p \neq 2, 7, \text{ then } p \equiv 1, 2, \text{ or } 4 \pmod{7}. \text{ If } 7 \mid N \text{ then } 7^2 \nmid N \end{aligned}$$

Start of lecture 13

Which integers are represented by $f(x, y) = x^2 + xy + 2y^2$? If $m, n \in \mathbb{Z}$, not both 0, then $m = dm_1$, $n = dn_1$, $d = \gcd(m, n)$, and then $(m_1, n_1) = 1$. So

$$f(m, n) = f(dm_1, dn_1) = d^2 f(m_1, n_1)$$

where $f(m_1, n_1)$ is properly represented by f. So $N \in \mathbb{N}$ is represented by $f \iff N = d^2 N_1$, $d, N_1 \in \mathbb{N}$, N_1 is properly represent by $f \iff$ if $p \mid N$ and $p \equiv 3$, 5 or 6 $\pmod{7}$, then p divides N an even number of times (i.e. e_p is even).

How general is this? Whenever $h(d) = 1$, there's a unique reduced PDBQF of discriminant d, and it represents N properly $\iff X^2 \equiv d \pmod{4N}$ is solvable. We can do a similar computation to characterise the integers represented by this reduced PDBQF in terms of congruence conditions on prime divisors.

If $h(d) > 1$, then we only have a criterion for N to be represented by some form of discriminant d. In fact, there do exist PDBQFs $f(x, y)$ such that the set of prime numbers p represented by f is not described by congruence conditions.

Example. $f(x, y) = x^2 + 23y^2$ (this is studied in Part III Algebraic Numer Theory).

The behaviour of $h(d)$ as $|d| \to \infty$ is well-studied.

- It's known that $h(d) \to \infty$ as $d \to -\infty$ (Siegel, Heilbrown, 1934).
- We know $h(d) = 1$ if and only if
$$d = -3, -4, -7, -8, -11, -19, -43, -67, -163$$
(Barker, Stark, 1967).

In Part II Number Fields, we define the ideal class group of a number field K. You can show that if $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, then there's a bijection between

$$\{\text{equivalence classes of PDBQF of discriminant } D\} \leftrightarrow \{\text{Ideal class group of } K.\}$$

$D =$ discriminant of $K = d$, if $d \neq k^2 d$, $k \in \mathbb{N}$, d_1 a discriminant.

4 Distribution of prime numbers

We know that there are infinitely many primes. We'd like to know: what's the probability that a 50-digit number if prime?

Theorem 4.1 (Prime Number Theorem)**.** For $X \geq 1$, define $\pi(x) = \#\{p \text{ prime} \mid p \leq x\}$. Then

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

as $x \to \infty$.

By definition, we say that $f \sim g$ if f, g are real-valued functions such that

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$$

So Prime Number Theorem says

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log(x)} = 1.$$

($\log x$ is logarithm to the base e).

It's easy to show that $\frac{x}{\log x} \sim \mathrm{li}(x)$, where

$$\mathrm{li}(x) := \int_{t=1}^{x} \frac{\mathrm{d}t}{\log t},$$

and in fact $\mathrm{li}(x)$ is a better approximation to $\pi(x)$ for large values of x.

So Prime Number Theorem is equivalent to $\pi(x) \sim \mathrm{li}(x)$ as $x \to \infty$. This says that the density of primes close to x is about $\frac{1}{\log(x)}$. So we expect that the probability that a random 20-digit number is prime to be about

$$\frac{1}{\log(5 \times 10^{19})} = 0.0220\ldots$$

The actual probability is

$$\frac{\pi(10^{20}) - \pi(10^{19})}{10^{20} - 10^{19}} = 0.0220\ldots$$

Nobody has yet computed $\pi(10^{50})$.

There are many variants of the Prime Number Theorem.

Theorem (Dirichlet's Theorem on Primes in Arithmetic Progression)**.** Take $a, N \in \mathbb{N}$, $N > 1$, $(a, N) = 1$. Then there are infinitely many primes p such that $p \equiv a \pmod{N}$.

Theorem 4.2. Let

$$\pi(a, N, x) = \#\{p \text{ prime} \mid p \leq x, p \equiv a \pmod{N}\}$$

Then if $a, N \in \mathbb{N}$, $N > 1$ and $(a, N) = 1$, then

$$\pi(a, N, x) \sim \frac{1}{\phi(N)} \frac{x}{\log x}$$

as $x \to \infty$.

Corollary. As $x \to \infty$, with appropriate conditions on a and N,

$$\frac{\pi(a, N, x)}{\pi(x)} \to \frac{1}{\phi(x)}.$$

"A randomly chosen prime lies in any possible congruence class modulo N with probability $\frac{1}{\phi(N)}$."

The proofs of these theorems are beyond the scope of this course. We will:

- Inrtoduce Riemann ζ-function and Dirichlet series (these are the main tools in the proofs of Theorem 4.1 and Theorem 4.2).
- Use elementary techniques to prove Chebyshev's Theorem:

$$\exists c_1, c_2 > 0 \; \forall x \geq 2, \qquad c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x}$$

Lemma 4.3. If $x \in \mathbb{N}$, $x > 2$, then

$$\pi(x) \geq \frac{\log x}{2 \log 2}.$$

Proof. Let $p_1, \dots, p_k$ be the primes $\leq x$. So $k = \pi(x)$. If $1 \leq n \leq x$, write $n = d^2 p_1^{\varepsilon_1} \cdots p_k^{\varepsilon_k}$, $d \in \mathbb{N}$, $\varepsilon_i \in \{0, 1\}$. Each such n has a unique expression in this form. We have $d \leq \sqrt{x}$. So

$$\begin{aligned} x = \#\{n \in \mathbb{Z} \mid 1 \leq n \leq x\} &\leq \sqrt{x} 2^{\pi(x)} \\ \implies \sqrt{x} &\leq 2^{\pi(x)} \\ \implies \frac{1}{2} \log x &\leq \pi(x) \log 2 \end{aligned}$$

□

Proposition 4.4.

(i) $\sum_{p \text{ prime}} \frac{1}{p}$ diverges.

(ii) $\prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right)^{-1}$ diverges.

Proof of (2) $\iff$ (1). Need to show

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} \to \infty$$

as $x \to \infty$. The logarithm of this is (recall that the Taylor series for $-\log(1-x)$ is absolutely convergent on $|x| < 1$, and $\frac{1}{p} < 1$):

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

Claim: $\sum_{p \le x} \sum_{k \ge 2} \frac{p^{-k}}{k}$ converges as $x \to \infty$. Enough to show these sums are bounded.

$$\begin{aligned}\sum_{p \le x} \sum_{k \ge 2} \frac{p^{-k}}{k} &\le \sum_{p \le x} \sum_{k \ge 2} p^{-k} \\ &= \sum_{p \le x} \frac{p^{-2}}{1 - \frac{1}{p}} \\ &= \sum_{p \le x} \frac{1}{p(p-1)} \\ &\le \sum_{n \ge 1} \frac{1}{n^2} \\ &< \infty\end{aligned}$$

So $\log \prod_{p \le x} \left(1 - \frac{1}{p}\right)^{-1} = \sum_{p \le x} \frac{1}{p} + f(x)$ where $f(x)$ converges as $x \to \infty$. So (1) $\iff$ (2). □

Start of lecture 14

Proof of (2).

$$\begin{aligned}\prod_{p \le x} \left(1 - \frac{1}{p}\right)^{-1} &= \prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \\ &= \sum_{k_1, \dots, k_r \ge 0} (p_1^{k_1} \cdots p_r^{k_r})^{-1}\end{aligned}$$

Every integer $1 \le n \le x$ is a product of primes $\le x$, so

$$\prod_{p \le x} \left(1 - \frac{1}{p}\right)^{-1} \ge \sum_{1 \le n \le x} \frac{1}{n} \to \infty$$

as $x \to \infty$ (harmonic series). □

Definition 4.5 (Riemann ζ)**.** The *Riemann ζ-function* is

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

Convention: $s \in \mathbb{C}$. This defines $\zeta(s)$ whenever this series converges.

$\zeta(s)$ studied by Euler for $s \in \mathbb{R}$ by Riemann for $s \in \mathbb{C} \to$ complex analysis.

Proposition 4.6. If $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$, then $\zeta(s)$ converges absolutely.

Notation. Notation: $s = \sigma + it$, $\sigma + it \in \mathbb{R}$.

Proof.
$$n^{-s} = \exp(-s \log n) = \exp(-(\sigma + it) \log n)$$
$$\implies |n^{-s}| = \exp(-\sigma \log n) = n^{-\sigma}$$
So $\sum_{n=1}^{\infty} |n^{-s}| = \sum_{n=1}^{\infty} n^{-\sigma}$. This converges if and only if $\sigma > 1$. □

Same arugument shows that $\zeta(s)$ converges uniformly in $\{s \in \mathbb{C} \mid \sigma > 1 + \delta\}$, for any $\delta > 0$. A uniform limit of holomorphic functions is holomorphic, so $\zeta(s)$ is holomorphic in $\{s \in \mathbb{C} \mid \sigma > 1\}$.

Theorem 4.7. If $s \in \mathbb{C}$, $\sigma > 1$, then
$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}.$$
More precisely
$$\lim_{x \to \infty} \prod_{p \le x} (1 - p^{-s})^{-1} = \zeta(s)$$
and this limit is non-zero.

Proof. Arguing informally, we have
$$\prod_p (1 - p^{-s})^{-1} = \prod_p (1 + p^{-s} + p^{-2s} + p^{-3s} + \cdots) = \sum_{n=1}^{\infty} n^{-s}.$$
By Fundamental Theorem of Arithmetic.

Arguing rigorously,
$$\prod_{p \le x} (1 - p^{-s})^{-1} = \sum_{k_1, \ldots, k_r} \ge 0 (p_1^{k_1} \cdots p_r^{k_r})^{-s}$$
where $p_1, \ldots, p_r$ are the primes $\le x$. Fundamental Theorem of Arithmetic implies if $n \in \mathbb{N}$, then n^{-s} apprears at most once in $\sum_{k_1, \ldots, k_r \ge 0} (p_1^{k_1} \cdots p_r^{k_r})^{-s}$, and exactly once if $n \le x$. So
$$\left| \prod_{p \le x} (1 - p^{-s})^{-1} - \zeta(s) \right| \le \sum_{n > x} n^{-\sigma} \to 0$$

as $x \to \infty$. So

$$\lim_{x\to\infty} p \leq x(1-p^{-s})^{-1} = \zeta(s).$$

To show $\zeta(s) \neq 0$, consider

$$\prod_{p\leq x}(1-p^{-s})\zeta(s) = \prod_{p>x}(1-p^{-s})^{-1} = 1 + \sum_{n\in S_x} n^{-s}$$

where

$$S_x = \{n \in \mathbb{N} \mid \text{all prime factors } p \mid n \text{ satisfy } p > x\} \subset \{n \in \mathbb{N} \mid n > x\}.$$

Then

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

Since $\sigma > 1$, $\sum_{n>x} n^{-\sigma} \to 0$ as $X \to \infty$, so we can choose x such that

$$1 - \sum_{n>x} n^{-\sigma} > 0.$$

Then we deduce that

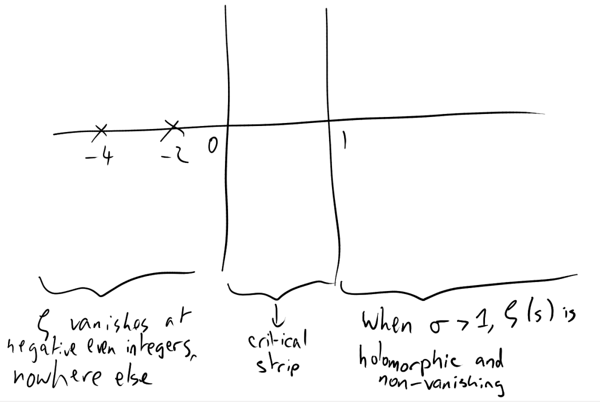
$$\left|\prod_{p\leq x}(1-p^{-s})\zeta(s)\right| \neq 0 \implies \zeta(s) \neq 0.$$ □

Non-examinable discussion of $\zeta(s)$

- Meromorphic continuation: $\zeta(s)$ admits a unique function on $\mathbb{C}$, with a simple polt at $s=1$, and no other poles.
- Functional equation: we define $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$, where $\Gamma(s)$ is the *Gamma function*, a meromorphic function in $\mathbb{C}$ defined for $\sigma > 0$ by the integral

  $$\Gamma(s) = \int_{y=0}^{\infty} e^{-y}y^s \frac{\mathrm{d}y}{y}.$$

  Then $\xi(s) = \xi(1-s)$.
- Trivial zeroes: $\xi(s)$ is meromorphic with simple poles at $s=0$, $s=1$ and no other poles. $\Gamma(s)$ has simple poles at $s = 0, -1, -2, \dots$ and no other poles. $\Gamma(s/2)$ has simple poles at $s = 0, -2, -4, \dots$. Since ξ is holomorphic at $s = -2, -4, -6, \dots$ but $\Gamma(s/2)$ has a pole, $\Gamma(s)$ must vanish, whenever s is a negative even integer (these are the trivial zeroes). Picture of $\zeta(s)$:



- Critical strip: this is the region $\{s \in \mathbb{C} \mid \sigma \in [0,1]\}$. All non-trivial zeroes of $\zeta(s)$ lie in the critical strip.

  Fact: their location is closely related to the distribution of primes. For example, the "hard part" in the proof of Prime Number Theorem (Theorem 4.1) is the non-existence of zeroes of $\zeta(s)$ with $\sigma = 1$.

  Conjecture 4.8 (Riemann Hypothesis)**.** If $s \in \mathbb{C}$ is a non-trivial zero of $\zeta(s)$, then $\sigma = \frac{1}{2}$.

  As stated in the first lecture, this is equivalent to the bound

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

  for any $x \geq 3$. Recall Prime Number Theorem says

$$\left| \frac{\pi(x)}{\mathrm{li}(x)} - 1 \right| \to 0$$

  as $x \to \infty$.

This is now the end of the non-examinable content.

Definition 4.9 (Dirichlet series)**.** A Dirichlet series is one of the form

$$\sum_{n=1}^{\infty} a_n n^{-s} \qquad a_n \in \mathbb{C}$$

Example. If $a_n = 1\ \forall n \in \mathbb{N}$, this is just $\zeta(s)$.

If $N \in \mathbb{N}$ is odd, then the Dirichlet series

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

plays a rule in the proof of Theorem 4.2 analogous to the role of $\zeta(s)$ in the proof of Theorem 4.1.

Remark. If $A, B > 0$ and $|a_n| \le An^B$ for all $n \ge 1$, then $\sum_{n=1}^{\infty} a_n n^{-s}$ converges absolutely whe $\sigma > 1 + B$.

Start of lecture 15

Dirichlet series are interesting when a_n is an arithmetically interesting sequence, and then $\sum_{n=1}^{\infty} a_n n^{-s}$ is a kind of generating function.

Definition (Dirichlet convolution)**.** The *Dirichlet convolution* of functions $f, g : \mathbb{N} \to \mathbb{C}$ is defined by

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

This satisfies the property that

$$\left(\sum_{n=1}^{\infty} f(n) n^{-s}\right)\left(\sum_{m=1}^{\infty} g(m) m^{-s}\right) = \sum_{n,m \ge 1} g(n) g(m) (nm)^{-s} = \sum_{n=1}^{\infty} h(n) n^{-s}.$$

Lemma 4.10. Let $f, g, h : \mathbb{N} \to \mathbb{C}$. Then:

(1) $f * g = g * f$ as functions $\mathbb{N} \to \mathbb{C}$.

(2) $(f * g) * h = f * (g * h)$.

(3) If f, g are mutliplicative (i.e. $f(mn) = f(m)f(n)$, $(m, n) = 1$) then $f * g$ is also multiplicative.

Proof.

(1)

$$(f * g)(n) = \sum_{d|} f(d) g\left(\frac{n}{d}\right) = \sum_{\substack{a,b \in \mathbb{N} \\ ab=n}} f(a)g(b).$$

This is symmetric in f and g.

(2)

$$\begin{aligned} ((f * g) * h)(n) &= \sum_{d_1 d_2 = n} (f * g)(d_1) h(d_2) \\ &= \sum_{d_1 d_2 = n} \sum_{e_1 e_2 = d_1} f(e_1) g(e_2) h(d_2) \\ &= \sum_{\substack{a,b,c \in \mathbb{N} \\ abc=n}} f(a)g(b)h(c) \end{aligned}$$

A computation shows this is equal to $(f * (g * h))(n)$.

(3) Let $m, n \in \mathbb{N}$, $(m, n) = 1$. Then

$$\begin{aligned} (f * g)(mn) &= \sum_{d|mn} f(d) g\left(\frac{mn}{d}\right) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2) g\left(\frac{mn}{d_1 d_2}\right) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2) g\left(\frac{m}{d_1}\right) g\left(\frac{m}{d_2}\right) \\ &= \left(\sum_{d_1|m} f(d_1) g\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2|n} f(d_2) g\left(\frac{n}{d_2}\right)\right) \\ &= (f * g)(m)(f * g)(n) \end{aligned}$$

□

Example.

$$\begin{aligned}\zeta(s-1)\zeta(s) &= \sum_{n=1}^{\infty} n^{1-s} \sum_{m=1}^{\infty} m^{-s} \\ &= \sum_{n=1}^{\infty} n \cdot n^{-s} \sum_{m=1}^{\infty} m^{-s} \\ &= \sum_{n=1}^{\infty} (f * g)(n) n^{-s} \\ &= \sum_{n=1}^{\infty} \sigma(n) n^{-s}\end{aligned}$$

where we use $f(n) = n$, $g(n) = 1$. Then $(f * g)(n) = \sum_{d|n} d = \sigma(n)$.

Definition 4.11 (Möbius function)**.** The Möbius function $\mu : \mathbb{N} \to \mathbb{C}$ is defined by

$$\mu(n) = \begin{cases} 0 & n \text{ is not squarefree} \\ (-1)^k & n = p_1 \cdots p_k,\ p_i \text{ distinct primes} \end{cases}$$

In particular, $\mu(1) = (-1)^0 = 1$.

Lemma 4.12. Let $\mathbb{1} : \mathbb{N} \to \mathbb{C}$ be $\mathbb{1}(n) = 1$ $\forall n \in \mathbb{N}$, and $\delta : \mathbb{N} \to \mathbb{C}$ be $\delta(n) = 1$ if $n = 1$, $\delta(n) = 0$ if $n > 1$. Then:

(1) δ is an identity for convolution: $\delta * f = f$, $\forall f : \mathbb{N} \to \mathbb{C}$.

(2) TODO

Proof.

(1) TODO

(2) TODO So it's enough to show $(\mu * \mathbb{1})(p^k) = \delta(p^k)$ if p is prime, $k \geq 0$. For $k = 0$:

$$(\mu * \mathbb{1})(p^k) = \sum_{d|1} \mu(d) = 1$$

For $k \geq 1$,

$$(\mu * \mathbb{1})(p^k) = \sum_{i=0}^{k} \mu(p^i) = \mu(1) + \mu(p) + \cdots + \mu(p^k) = 1 - 1 + 0 \cdots + 0 = 0 = \delta(p^k). \quad \square$$

Proposition 4.13 (Möbius inversion formula)**.** Suppose $f, g : \mathbb{N} \to \mathbb{C}$ are such that

$$f(n) = \sum_{d|n} g(d) \qquad \forall n \in \mathbb{N}$$

Then

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) \qquad \forall n \in \mathbb{N}$$

Proof. By definition, we have $f = g * \mathbb{1}$, and we need to show $g = \mu * f$. But $\mu * f = \mu * g * \mathbb{1} = g * (\mathbb{1} * \mu) = g * \delta = g$. □

Definition 4.14 (von Mongoldt function)**.** The von Mongoldt function $\Lambda : \mathbb{N} \to \mathbb{C}$ is defined by

$$\Lambda(n) = \begin{cases} 0 & \text{if } n \text{ is not a prime power} \\ \log p & \text{if } n = p^k,\ p \text{ prime},\ k \geq 1 \end{cases}$$

"Weighted indicator function" of prime powers.

The Chebyshev function $\psi : [1, \infty) \to \mathbb{C}$ is defined by $\psi(x) = \sum_{1 \leq n \leq x} \Lambda(n) = \sum_{p^k \leq x} \log p$. One can show using elementary methods that

$$\psi(x) \sim \pi(x) \log(x)$$

where $\pi(x)$ is the prime counting function as usual. Recall Theorem 4.1 (Prime Number Theorem) says that $\pi(x) \sim \frac{x}{\log x}$ as $x \to \infty$. This is equivalent to saying that

$$\psi(x) \sim x$$

as $x \to \infty$ (i.e. $\lim_{x \to \infty} \frac{\psi(x)}{x} = 1$).

Theorem 4.15. If $s \in \mathbb{C}$, $\sigma = \mathrm{Re}(s) > 1$, then

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

Proof. Both LHS and RHS are holomorphic, so it's enough to show equality when $s = \sigma$

is real (identity principle for holomorphic functions).

$$\begin{aligned}
-\frac{\zeta'(s)}{\zeta(s)} &= -\frac{\mathrm{d}}{\mathrm{d}\sigma}\log\zeta(\sigma) \\
&= -\frac{\mathrm{d}}{\mathrm{d}\sigma}\log\prod_p(1-p^{-\sigma})^{-1} \\
&= -\frac{\mathrm{d}}{\mathrm{d}\sigma}\sum_p -\log(1-p^{-\sigma}) \\
&= -\frac{\mathrm{d}}{\mathrm{d}\sigma}\sum_p\sum_{k\geq 1}\frac{p^{-k\sigma}}{k}
\end{aligned}$$

Using $-\log(1-x) = \sum_{k\geq 1}\frac{x^k}{k}$, $|x| < 1$. We can interchange order of differentiation and summation, using uniform convergence. So

$$\begin{aligned}
-\frac{\zeta'(\sigma)}{\zeta(\sigma)} & \\
&= -\sum_{\substack{p \text{ prime} \\ k\geq 1}}\frac{\mathrm{d}}{\mathrm{d}\sigma}\frac{p^{-k\sigma}}{k} \\
&= -\sum_p \frac{\mathrm{d}}{\mathrm{d}\sigma}\frac{\exp(-k\sigma\log p)}{k} \\
&= \sum_{\substack{p \\ k\geq 1}}(\log p)p^{-k\sigma} \\
&= \sum_{n=1}^{\infty}\Lambda(n)n^{-\sigma}
\end{aligned}$$

□

What happens next? If $\zeta(s)$ has a zero of order k at $s = s_0$, then $-\frac{\zeta'(s)}{\zeta(s)}$ will have a simple pole at $s = s_0$ of residue $-k$. You can consider a contour integral of $-\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{x}$ and evaluate using Cauchy's residue theorem to prove a formula

$$\psi(x) = x - \sum_\rho \frac{x^\rho}{\rho} - \frac{\zeta'(0)}{\zeta(0)}$$

valid when $x > 2$ is not a prime power, where the sum $\sum_\rho$ is over zeroes ρ of the Riemann ζ-function. "Riemann's explicit relation".

We now turn to elementary techniques to study the distribution of primes. Main goal: Chebyshev's Theorem:

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

Main tool: prime factorisation of binomial coefficients $\binom{2n}{n}$, $n \in \mathbb{N}$.

Start of lecture 16

Proposition 4.16 (Legendre's Formula)**.** Let $X > 1$. Then

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

where

$$P = \prod_{\substack{p \leq \sqrt{x} \\ \text{prime}}} p,$$

and μ is the Möbius function.

Proof. If $n \in \mathbb{N}$, $n > 1$, $n \leq x$, then n is prime if and only if there does not exist a prime $q \leq \sqrt{x}$ such that $q \mid n$ (if $n = ab$ with $a \leq b$ then $a \leq \sqrt{x}$). So

$$\begin{aligned} \{1 \leq n \leq x \mid (n, P) = 1\} &= \{1\} \cup \{p \leq x \text{ prime} \mid (p, P) = 1\} \\ &= \{1\} \cup \{p \leq x \text{ prime} \mid p > \sqrt{x}\} \end{aligned}$$

and

$$\#\{1 \leq n \leq x \mid (n, P) = 1\} = 1 + \pi(x) - \pi(\sqrt{x}).$$

Last time we showed that if $n \in \mathbb{N}$, then

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

So

$$\begin{aligned} \#\{1 \leq n \leq x \mid (n, P) = 1\} &= \sum_{1 \leq n \leq x} \sum_{d \mid (n, P)} \mu(d) \\ &= \sum_{d \mid P} \mu(d) \sum_{\substack{1 \leq n \leq x \\ d \mid n}} 1 \\ &= \sum_{d \mid P} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor \end{aligned}$$

□

Definition 4.17. Let $N \in \mathbb{N}$, p a prime number. Then

$$\nu_p(N) = p\text{-adic valuation of } N = \text{exponent of } p \text{ in prime factorisation of } N.$$

So $N = p^{\nu_p(N)} N_1$, $N_1 \in \mathbb{N}$, $(p, N_1) = 1$.

Note. $\nu_p(N) = 0 \iff p \nmid N$. If $N, M \in \mathbb{N}$, then $\nu_p(NM) = \nu_p(N) + \nu_p(M)$.

Lemma 4.18. Let $n \in \mathbb{N}$, $N = \binom{2n}{n} = \frac{(2n)!}{(n!)^2}$. Then:

(1) $\frac{2^{2n}}{2n} \leq N < 2^{2n}$.

(2) If p is prime, and $n < p \leq 2n$, then $\nu_p(N) = 1$.

(3) If p is an odd prime, and $\frac{2n}{3} < p \leq n$, then $\nu_p(N) = 0$.

(4) For any prime p, $p^{\nu_p(N)} \leq 2n$.

Proof.

(1) $2^{2n} = (1+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} = 2 + \sum_{i=1}^{2n-1} \binom{2n}{i} \geq 2 + \binom{2n}{n} = 2 + N$. Hence $N < 2^{2n}$. If $1 \leq i \leq 2n-1$, then $\binom{2n}{i} \leq \binom{2n}{n}$. So

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

Therefore $N \geq \frac{2^{2n}}{2n}$.

(2)

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

$n < p \leq 2n \implies p$ does not divide the denominator. Also, there's exactly one multiple of p in the numerator, namely p itself. So

$$\nu_p(N) = \underbrace{\nu_p((2n)\cdots(n+1))}_{=1} - \underbrace{\nu_p(n(n-1)\cdots(1))}_{=0}.$$

(3) Now p is an odd prime with $\frac{2n}{3} < p \leq n$. So $\frac{4n}{3} < 2p \leq 2n$, $2n < 3p$. So in

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

the only multiple of p in the denominator is p, and the only multiple of p in the numerator is $2p$. So

$$\nu_p(N) = \nu_p(2p) - \nu_p(p) = 1 - 1 = 0$$

as p is odd.

(4) We will use the formula ($n \in \mathbb{N}$, p prime),

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

(to be proved on Example Sheet 3). Note the sum is finite as when $p^i > n$, $\frac{n}{p^i} < 1$ so $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$. We want to show that $p^{\nu_p(N)} \le 2n$, or that is $k \ge 0$, and $p^k \mid N$, then $p^k \le 2n$. We'll show instead that if $p^k > 2n$, then $p^k \nmid N$. We have

$$\begin{aligned} \nu_p(N) &= \nu_p((2n)!) - 2\nu_p(n!) \\ &= \sum_{i=1}^{\infty} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^2} \right\rfloor \right) \end{aligned}$$

If $p^k > 2n$, then this equals

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

(since if $i \ge k$ then $p^i > 2n \implies \frac{2n}{p_i} < 1$, so $\left\lfloor \frac{2n}{p^i} \right\rfloor = 0$). If $x \in \mathbb{R}$, $x > 0$, then $\lfloor 2x \rfloor - 2 \lfloor x \rfloor \in \{0, 1\}$. Why? If $x = m + \alpha$, $m \in \mathbb{Z}$, $\alpha \in [0, 1)$, then $\lfloor x \rfloor = m$, $2x = 2m + 2\alpha$, so

$$\lfloor 2x \rfloor = \begin{cases} 2m & \alpha \in \left[0, \frac{1}{2}\right) \\ 2m + 1 & \alpha \in \left[\frac{1}{2}, 1\right) \end{cases}$$

So

$$\lfloor 2x \rfloor - 2 \lfloor x \rfloor = \begin{cases} 0 & \alpha \in \left[0, \frac{1}{2}\right) \\ 1 & \alpha \in \left[\frac{1}{2}, 1\right) \end{cases}$$

So

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

So $p^k \nmid N$. □

Theorem 4.19 (Chebyshev's Theorem)**.** There exist $c_1, c_2 > 0$ such that $\forall x > 4$,

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

The proof will show we can take $c_1 = \frac{\log 2}{2}$, $c_2 = 6 \log 2$.

Proof. Strategy: prove bounds that work for certain integer values of x, and then interpolate to all $x > 4$.

We first prove the upper bound.

Claim: If $k \geq 1$, $\pi(2^k) \leq \frac{3 \times 2^k}{k}$. Note that if $n \in \mathbb{N}$, then $\pi(2n) \leq n$ (as primes are among $2, 3, 5, 6, \ldots$). We have

$$\frac{2^k}{k} = 2^{k-1} \leq \frac{3 \times 2^k}{k} \iff k \leq 6.$$

So the claim holds if $k \leq 6$. Now suppose the claim holds for some $k \geq 5$, and let $n = 2^k$, $N = \binom{2n}{n}$. Then

$$\begin{aligned} 2^{2n} &> N && \text{(Lemma 4.18(1))} \\ &\geq \prod_{\substack{n<p\leq 2n \\ p \text{ prime}}} p && \text{(Lemma 4.18(2))} \\ &\geq \prod_{\substack{n<p\leq 2n \\ p \text{ prime}}} n && (p \geq n) \\ &= n^{\pi(2n)-\pi(n)} \end{aligned}$$

So

$$\pi(2n) - \pi(n) = \pi(2^{k+1}) - \pi(2^k) \leq \frac{\log 2^{2n}}{\log n} = \frac{2n \log 2}{\log 2^k} = \frac{2^{k+1}}{k}.$$

Rearrange:

$$\pi(2^k + 1) \leq \pi(2^k) + \frac{2^{k+1}}{k} \leq \frac{3 \times 2^k}{k} + \frac{2^{k+1}}{k} = \frac{5 \cdot 2^k}{k}$$

We have

$$\frac{5 \times 2^k}{k} \leq \frac{3 \times 2^{k+1}}{k+1} \iff 5(k+1) \leq 6k \iff k \geq 5$$

This proves the claim. Rest of proof next time.

Start of lecture 17

Suppose $x > 4$, and $2^k \leq x < 2^{k+1}$, for some $k \geq 2$. Then

$$\pi(x) \leq \pi(2^{k+1}) \leq \frac{3 \times 2^{k+1}}{k+1} \leq \frac{6 \times 2^k}{k} = 6 \log 2 \cdot \frac{2^k}{k \log 2} = 6 \log 2 \cdot f(2^k)$$

where $f(x) = \frac{x}{\log x}$. Note that

$$f'(x) = \frac{\log x - 1}{(\log x)^2}$$

and $f'(x) > 0$ when $x > e$. Hence $f(x)$ is increasing on $(4, \infty)$. Hence

$$\pi(x) \leq 6 \log 2 \cdot f(x) = 6 \log 2 \frac{x}{\log x}.$$

We now find a lower bound for $\pi(x)$. Let $n \in \mathbb{N}$, $N = \binom{2n}{n}$. We know if p is a prime and $p \mid N$, then $p \leq 2n$. So

$$N = \prod_p p^{\nu_p(N)} = \prod_{p \leq 2n} p^{\nu_p(N)} \leq \prod_{p \leq 2n} (2n) = (2n)^{\pi(2n)}.$$

We also know that $N \geq \frac{2^{2n}}{2n}$, hence

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

Hence

$$\begin{aligned} &\implies 2^{2n} \leq (2n)^{\pi(2n)+1} \\ &\implies 2n \log 2 \leq (\pi(2n) + 1) \log 2n \\ &\implies \pi(2n) \geq \frac{2n}{\log 2n} \cdot \log 2 - 1 \end{aligned}$$

Now suppose $X > 4$, and choose $n \in \mathbb{N}$ so that $2n \leq x \leq 2n + 2$. Then

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

Claim: If $x \geq 16$, then

$$\frac{x-2}{\log x} \log 2 - 1 \geq \frac{x}{\log x} \frac{\log 2}{2}.$$

Proof of the claim: Equivalent to

$$\frac{\log 2}{2} \frac{x}{\log x} - \frac{2 \log 2}{\log x} - 1 \geq 0 \tag{$*$}$$

Plugging in $x = 16$, we get

$$\frac{\log 2}{2} \cdot \frac{16}{4 \log 2} - \frac{2 \log 2}{4 \log 2} - 1 = 2 - \frac{1}{2} - 1 = \frac{1}{2} \geq 0.$$

Note the RHS of $(*)$ is increasing when $x \geq 16$.

This claim now implies

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

when $x \geq 16$. Remains to consider $4 < x \leq 16$. $\frac{x}{\log x}$ is increasing implies the largest value of $\frac{\log 2}{2} \frac{x}{\log x}$ in thsi range is

$$\frac{\log 2}{2} \cdot \frac{16}{4 \log 2} = 2.$$

Certainly $\pi(x) \geq 2$ when $4 < x \leq 16$. $\square$

Theorem 4.20 (Bertrand's Postulate)**.** If $n \in \mathbb{N}$, $n > 1$, then there exists a prime p such that $n \leq p < 2n$.

We first prove:

Lemma 4.21. Let $x \geq 1$, $P(x) = \prod_{p \leq x} p$. Then $P(x) \leq 4^x$.

Proof. It suffices to show $P(x) \leq 4^x$ when $x = n \in \mathbb{N}$. We do this b induction on n. It holds for $n = 1, 2$. For the finduction step, consider for $k \in \mathbb{N}$,

$$2\binom{2k+1}{k+1} = \binom{2k+1}{k+1} + \binom{2k+1}{k} \leq (1+1)^{2k+1} = 2^{2k+1}.$$

If p is a prime and $k + 2 \leq p \leq 2k + 1$, then $p \mid \binom{2k+1}{k+1}$. So

$$P(2k+2) = P(2k+1) = \prod_{p \leq 2k+1} p = \prod_{p \leq k+1} p \prod_{k+2 \leq p \leq 2k+1} p.$$

By induction,

$$P(2k+1) \leq 4^{k+1}\binom{2k+1}{k+1} \leq 4^{k+1}4^k = 4^{2k+1}.$$

Hence, $P(2k+1) \leq 4^{2k+1}$, and $P(2k+2) = P(2k+1) \leq 4^{2k+1} \leq 4^{2k+2}$. □

Proof of Theorem 4.20. Let $n \in \mathbb{N}$, $n > 1$, and suppose for contradiction that there are no primes p with $n \leq p < 2n$. Consider $N = \binom{2n}{n}$. We proved in Lemma 4.18 that if $p \mid N$, then either $p > n$ or $p \leq \frac{2n}{3}$. So in fact (since we're assuming there are no primes between n and $2n$),

$$N = \prod_{p \leq \frac{2n}{3}} p^{\nu_p(N)}.$$

Write $N = N_1 N_2$, where

$$N_1 = \prod_{\substack{p \mid N \\ \nu_p(N)=1}}, \qquad N_2 = \prod_{p \mid N \nu_p(N) \geq 2} p^{\nu_p(N)}.$$

By Lemma 4.21, we have

$$N_1 \leq P\left(\frac{2n}{3}\right) \leq 4^{\frac{2n}{3}}.$$

If p is prime and $\nu_p(N) \geq 2$, then (by Lemma 4.18), $p^{\nu_p(N)} \leq 2n \implies p \leq \sqrt{2n}$. So

$$\frac{2^{2n}}{2n} \leq N = N_1 N_2 \leq 4^{\frac{2n}{3}} (2n)^{\sqrt{2n}}.$$

(as product over primes $p \leq \sqrt{2n}$). Rearrange:

$$\begin{aligned} 2^{2n} - \frac{4n}{3} &\leq (2n)^{1+\sqrt{2n}} \\ \implies \frac{2n}{3} \log 2 &\leq (1 + \sqrt{n}) \log 2n \end{aligned}$$

This is a contradiction when n is large enough (as $\frac{(1+\sqrt{2n}) \log 2n}{2n} \to 0$ as $n \to \infty$). In fact, this gives a contradiction when $n \geq 500$, so the theorem holds in this case. To complete the proof for $1 < n < 500$, can either check every case by hand, or note that it's enough to find a sequence $2 = p_1, p_2, \dots, p_r$ of primes such that:

- $\forall i = 1, \dots, r-1$, $p_{i+1} \leq 2p_i + 1$.
- $p_r < 500$.

(as then the intervals $\left(\frac{p}{2}, p\right]$ cover $\mathbb{N} \cap (1, 500)$).

We can take $2, 5, 11, 23, 47, 89, 179, 359, 719$. □

Start of

lecture 18

5 Continued Fractions

$\alpha \in \mathbb{R} \to$ decimal expansion $\alpha = \sum \frac{a_i}{10^i}$, $a_i \in \{0, 1, 2, \ldots, 9\}$. Useful properties: if $\alpha, \beta \in \mathbb{R}$ are distinct then it's easy to decide whether $\alpha < \beta$ or $\alpha > \beta$ if you know their decimal expansions.

Continued fractions give another way of representing real numbers by sequences of integers. Useful properties: allow us to find good rational approximations for $\alpha \in \mathbb{R}$. For example, for $\alpha = \pi$:

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

The second approximation is "better", as it's closer to π and 113 is much smaller than 100000. $\frac{355}{113}$ is a truncation of the continued fraction expansion of π.

Notation. Suppose $a_0, \ldots, a_n \in \mathbb{R}$, $a_i > 0$ if $i > 0$. Then

$$[a_0, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \frac{1}{a_n}}}}$$

A continued fraction.

So $[a_0, a_1] = a_0 + \frac{1}{a_1}$, $[a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = [a_0, [a_1, a_2]]$. In general, $[a_0, \ldots, a_n] = [a_0, \ldots, a_{i-1}, [a_i, \ldots, a_n]]$ for any $1 \le i \le n$. Continued fraction algorithm: start with $\theta \in \mathbb{R}$. Produce a sequence $a_0, a_1, \ldots$ of integers with $a_i \geq 1$ and a sequence $\theta = \theta_0, \theta_1, \theta_2, \ldots$ of real numbers such that if θ_{n+1} is defined for $n \geq 0$, then $\theta = [a_0, a_1, \ldots, a_n, \theta_{n+1}]$. Either the algorithm will terminate: get finite sequence $a_0, \ldots, a_n, \theta_{n-1} = a_n$ such that $\theta = [a_0, \ldots, a_n]$.

Or the algorithm does not terminate: then sequence $(a_i)_{i \geq 0}$ is infinite and we write finally $\theta = [a_0, a_1, a_2, \ldots]$ and call this the continued fraction expansion of θ. We'll show later that in this case,

$$\theta = \lim_{n \to \infty} [a_0, \ldots, a_n].$$

Step 0: $\theta = \theta_0$. Set $a_0 = \lfloor \theta_0 \rfloor$. If $a_0 = \theta_0$ then stop. Otherwise, $0 < \theta_0 - a_0 < 1 \implies$ if we set $\theta_1 = \frac{1}{\theta_0 - a_0}$, then $\theta_1 > 1$ and $\theta = [a_0, \theta_1]$.

Step 1: set $a_1 = \lfloor \theta_1 \rfloor$. If $a_1 = \theta_1$ then stop (and $\theta = [a_0, a_1]$). Otherwise, $0 < \theta_1 - a_1 < 1$, so if we set $\theta_2 = \frac{1}{\theta_1 - a_1}$, then $\theta_2 > 1$ and $\theta = [a_0, [a_1, \theta_2]] = [a_0, a_1, \theta_2]$.

Step n, $n \geq 1$: Set $a_n = \lfloor \theta_n \rfloor \geq 1$, as $\theta_n > 1$. If $a_n = \theta_n$ then stop (and then $\theta = [a_0, \dots, \theta_n] = [a_0, \dots, a_n]$). Otherwise, $0 < \theta_n - a_n < 1$, so if we set $\theta_{n+1} = \frac{1}{\theta_n - a_n}$, then $\theta_{n+1} > 1$ and $\theta = [a_0, \dots, a_{n-1}, \theta_n] = [a_0, \dots, a_{n-1}, [a_n, \theta_{n+1}]] = [a_0, \dots, a_n, \theta_{n+1}]$.

Notation. $(a_i)_{i \geq 0}$ are called the partial quotients of $\theta \in \mathbb{R}$.

So $\theta_1 = \frac{c_1}{c_2}$, where $c_1, c_2 \in \mathbb{N}$, $c_1 > c_2$, $(c_1, c_2) = 1$. Apply Euclid's algorithm to c_1, c_2. Get:

$$\begin{aligned} c_1 &= d_1 c_2 + c_3 & c_2 &> c_3 > 0 \\ c_2 &= d_2 c_3 + c_4 & c_3 &> c_4 > 0 \\ &\vdots \\ c_{n-1} &= d_{n-1} c_n + c_{n+1} & c_n &> c_{n+1} > 0 \\ c_n &= d_n c_{n+1} & c_{n+1} &= 1, c_{n+2} = 0 \end{aligned}$$

Claim. If $1 \leq i \leq n$, then $\theta_i = \frac{c_i}{c_{i+1}}$. (In particular, continued fraction algorithm doesn't terminate before Step n).

If $i = 1$, $\theta_1 = \frac{c_1}{c_2}$. If $\theta_i = \frac{c_i}{c_{i+1}}$, $i < n$, then $c_i = d_i c_{i+1} + c_{i+2}$. Hence

$$\frac{c_i}{c_{i+1}} = \theta_i = d_i + \frac{c_{i+2}}{c_{i+1}}, \qquad \frac{c_{i+2}}{c_{i+1}} < 1.$$

So $a_i = \lfloor \theta_i \rfloor = d_i$, $\theta_{i+1} = \frac{1}{\theta_i - a_i} = \frac{c_{i+1}}{c_{i+2}}$. So the claim is true by induction.

Algorithm terminates at step n: $\theta_n = \frac{c_n}{c_{n+1}} = d_n \in \mathbb{Z}$ hence $\lfloor \theta_n \rfloor = \theta_n = a_n$. □

Definition 5.1. Suppose $(a_i)_{i \geq 0}$ is a sequence of integers, $a_i \geq 1$ if $i \geq 1$. Then we define sequences $(p_n)_{n \geq 0}$, $(q_n)_{n \geq 0}$ recursively by

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

for $n \geq 2$.

Remark.

(1) We can define $p_{-1} = 1$, $q_{-1} = 0$. Then the recurrence relation holds also for $n = 1$.

(2) We can write the recurrence relation as a matrix equation:

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

Hence

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}$$

(3) The sequenc e0 $< q_1 < q_2 < q_3 < \cdots$ is strictly increasing, as $a_n \geq 1$ when $n \geq 1$. Hence $q_n \geq q_{n-1} + q_{n-2}$ when $n \geq 1$.

(4) If $[a_0, a_1, \dots]$ is the continued fraction expansion of $\theta \in \mathbb{R}$, then $\left(\frac{p_n}{q_n}\right)_{n \geq 0}$ is called the sequence of convergents of θ.

Proposition 5.2. $(a_i)_{i \geq 0}$ sequence of integers, $a_i \geq 1$ if $i \geq 1$. Then:

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

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

(3) If $\beta \in \mathbb{R}$, $\beta > 0$ and $n \geq 0$, then

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

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

Important special case: If θ has continued fraction expansion $[a_0, a_1, \dots]$ then

$$\theta = [a_0, \dots, a_n, \theta_{n+1}] = \frac{\theta_{n+1} p_n + p_{n-1}}{\theta_{n+1} q_n + q_{n-1}}.$$

Proof.

(1) Follows from (3) (case $\beta = a_{n+1}$).

(2) Take determinants in the matrix expression for

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$$

and we deduce $p_n q_{n-1} - q_{n-1} q_n = (-1)^{n-1}$. This shows $(p_n, q_n) = 1$ and

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

Start of lecture 19

(3) Induction on n. $n = 0$: $[a_0, \beta] = a_0 + \frac{1}{\beta} = \frac{\beta a_0 + 1}{\beta}$. In general, $[a_0, \ldots, a_{n+1}, \beta] = [a_0, \ldots, a_n, [a_{n+1}, \beta]] = [a_0, \ldots, a_n, \gamma]$, where $\gamma = [a_{n+1}, \beta]$. By induction, this is

$$\frac{\gamma p_n + p_{n-1}}{\gamma q_n + q_{n-1}} = \frac{a_{n+1} p_n + \beta^{-1} p_n + p_{n-1}}{a_{n+1} q_n + \beta^{-1} q_n + q_{n-1}} = \frac{p_{n+1} + \beta^{-1} p_n}{q_{n+1} + \beta^{-1} q_n} = \frac{\beta p_{n+1} + p_n}{\beta q_{n+1} + q_n}.$$

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

Simple fact: if $x, y, x;, y' \in \mathbb{R}$, $y, y' > 0$, $\frac{x}{y} < \frac{x'}{y'}$, then

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

Here: take

$$\frac{x}{y} = \min\left(\frac{\beta p_n}{\beta q_n}, \frac{p_{n-1}}{q_{n-1}}\right) \qquad \frac{x'}{y'} = \max\left(\frac{\beta p_n}{\beta q_n}, \frac{p_{n-1}}{q_{n-1}}\right)$$

□

Theorem 5.3. Let $\theta \in \mathbb{R} \setminus \mathbb{Q}$, $\theta = [a_0, a_1, a_2, \ldots]$. Then:

(1) $\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}$ for all $n \geq 0$.

(2) $\lim_{n\to\infty} \frac{p_n}{q_n} = \lim_{n\to\infty} [a_0, \ldots, a_n] = \theta$.

Reminder: $\frac{p_n}{q_n}$ are called the convergents of $[a_0, a_1, \ldots]$.

Proof. We know $\theta = [a_1, a_2, \ldots, a_{n+1}, \theta_{n+2}]$ for all $n \geq 0$. So

$$\theta = \frac{\theta_{n+2} p_{n+1} + p_n}{\theta_{n+2} q_{n+1} + q_n}$$

lies strictly between $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$. Therefore

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

(inequality must be strict as $\theta \notin \mathbb{Q}$). We've observed that $0 < q_1 < q_2 < \cdots$, so $q_n \to \infty$ as $n \to \infty$. ☐

Remark. You can show that $\theta \mapsto [a_0, a_1, \dots]$ induces a bijection

$$\mathbb{R} \setminus \mathbb{Q} \xrightarrow{\sim} \mathbb{Z} \times \mathbb{N}^{\mathbb{N}}.$$

Example. $\pi = [3, 7, 15, 1, 292, 1, \dots]$. First few convergents:

$$\begin{aligned} [3] &= \frac{3}{1} \\ [3, 7] &= \frac{22}{7} \\ [3, 7, 15] &= \frac{333}{106} \\ [3, 7, 15, 1] &= \frac{355}{113} \end{aligned}$$

We now prove two theorems making precise the sense in which the convergents of $\theta \in \mathbb{R} \setminus \mathbb{Q}$ give a sequence of "best possible" rational approximations to θ.

Theorem 5.4. Let $\theta \in \mathbb{R} \setminus \mathbb{Q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$. Then:

(1) If $q < q_{n+1}$, then $|q\theta - p| \geq |q_n\theta - p_n|$.

(2) If $\left|\theta - \frac{p}{q}\right| < \left|\theta - \frac{p_n}{q_n}\right|$, then $q > q_n$.

Proof. First prove (1) $\implies$ (2): Suppose $q \leq q_n$. Then $q < q_{n+1}$, so $|q\theta - p| \geq |q_n\theta - p_n|$. So

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

Now we prove (1): there exist integers $u, v \in \mathbb{Z}$ such that

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

since

$$\det \begin{pmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{pmatrix} \in \{\pm 1\}$$

we can invert the matrix over integers. Then

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

If $v = 0$, then $|q\theta - p| = |u||q_n\theta - p_n|$. u is a non-negative integer, so

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

If $v \neq 0$, then $q = q_{n+1}v + q_n u$ and $q < q_{n+1}$. Hence u, v must have opposite signs, with $u \neq 0$. The sign of $q_n\theta - p_n$ is the same as the sign of $\theta - \frac{p_n}{q_n}$, which is the oppositve of the sign of $\theta - \frac{p_{n+1}}{q_{n+1}}$. Therefore $u(q_n\theta - p_n)$ and $v(q_{n+1}\theta - p_{n+1})$ have the same sign. Therefore

$$\begin{aligned} |q\theta - p| &= |u||q_n\theta - p_n| + |v||q_{n+1}\theta - p_{n+1}| \\ &\geq |q_n\theta - p_n| \end{aligned}$$

as $u \neq 0$. □

Theorem 5.5. Let $\theta \in \mathbb{R} \setminus \mathbb{Q}$. Then

(1) For all $n \geq 0$, there exists $\frac{p}{q} \in \{\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}\}$ such that

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

(2) If $p \in \mathbb{Z}$, $q \in \mathbb{N}$, and $\left|\theta - \frac{p}{q}\right| < \frac{1}{2q^2}$, then $\frac{p}{q}$ is a convergent of θ.

Proof.

(1) Again use that $\theta - \frac{p_n}{q_n}, \theta - \frac{p_{n+1}}{q_{n+1}}$ has opposite sign. Hence

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

So we have $\left|\theta - \frac{p_i}{q_i}\right| < \frac{1}{2q_i^2}$ for at least one $i \in \{n, n+1\}$. α, β distinct, positive real numbers. Therefore

$$(\alpha - \beta)^2 > 0 \implies \frac{1}{2}(\alpha^2 + \beta^2) > \alpha\beta.$$

(2) Choose $n \geq 0$ soc that $q_n \leq q < q_{n+1}$. Then $|q\theta - p| \geq |q_n\theta - p_n|$, by Theorem 5.4(1). We consider

$$\begin{aligned}
\left|\frac{p}{q} - \frac{p_n}{q_n}\right| &\leq \left|\theta - \frac{p}{q}\right| + \left|\theta - \frac{p_n}{q_n}\right| \\
&= \frac{1}{q}|q\theta - p| + \frac{1}{q_n}|q_n\theta - p_n| \\
&\leq \left(\frac{1}{q} + \frac{1}{q_n}\right)(q\theta - p) \\
&< \left(\frac{1}{q} + \frac{1}{q_n}\right)\frac{1}{2q}
\end{aligned}$$

Suppose for contradiction that $\frac{p}{q} \neq \frac{p_n}{q_n}$. Then

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

so

$$\begin{aligned}
\frac{1}{qq_n} < \left(\frac{1}{q} + \frac{1}{q_n}\right) &\implies \frac{1}{q_n} < \frac{1}{2q} + \frac{1}{2q_n} \\
&\implies \frac{1}{2q_n} < \frac{1}{2q} \\
&\implies q < q_n ※
\end{aligned}$$

□

Application: If $d \in \mathbb{N}$ is a non-square, can find solutions to *Pell's equation* $x^2 - dy^2 = 1$, with $x, y \in \mathbb{N}$? If (p, q) is a solution, then

$$\begin{aligned}
&\left(\frac{p}{q}\right)^2 - d = \frac{1}{q^2} \\
\implies &\frac{p}{q} - \sqrt{d} = \frac{1}{q^2}\frac{1}{\frac{p}{q} + \sqrt{d}} < \frac{1}{2q^2} \\
\implies &\frac{p}{q} \text{ is a convergent of} \sqrt{d} \in \mathbb{R} \setminus \mathbb{Q}
\end{aligned}$$

Start of lecture 20

We now study the continued fraction expansions of *quadratic irrationals* $\theta \in \mathbb{R} \setminus \mathbb{Q}$: i.e. irrational θ such that θ satisfies an equation

$$a\theta^2 + b\theta + c = 0 \qquad a, b, c \in \mathbb{Z}.$$

(or equivalently θ of the form $r + s\sqrt{d}$, $r, s \in \mathbb{Q}$, $s \neq 0$, $d \in \mathbb{N}$ not a square).

Example. $d = 6$, $\theta = \sqrt{6}$. $2 < \sqrt{6} < 3$ so $a_0 = \lfloor\sqrt{6}\rfloor = 2$, $\theta_1 = \frac{1}{\sqrt{6}-2} = \frac{\sqrt{6}+2}{2} = \frac{\sqrt{6}-2}{2}+2$. Hence $a_1 = \lfloor\theta_1\rfloor = 2$, $\theta_2 = \frac{2}{\sqrt{6}-2} = \sqrt{6}+2 = (\sqrt{6}-2)+4$, so $a_2 = \lfloor\theta_2\rfloor = 4$, $\theta_3 = \frac{1}{\sqrt{6}-2} = \theta_1$. So

$$\begin{aligned}\theta &= [a_0, \theta_1] \\ &= [a_0, a_1, \theta_2] \\ &= [a_0, a_1, a_2, a_1, a_2, \theta_1] \\ &= [2, 2, 4, 2, 4, 2, 4, \dots] \\ &= [2, \overline{2, 4}]\end{aligned}$$

(overline means repeat this pattern indefinitely).

Definition (Essentially periodic)**.** Let $\theta \in \mathbb{R} \setminus \mathbb{Q}$ have continued fraction expansion $[a_0, a_1, a_2, \dots]$. Then the continued fraction expansion of θ is *essentially periodic* of period k if it has the form $[a_0, a_1, \dots, a_{m-1}, \overline{a_m, \dots, a_{m+k-1}}]$. It is *purely periodic* if we can take $m = 0$.

Example. continued fraction expansion of $\sqrt{6}$ is essentially periodic; continued fraction expansion of $\frac{1}{\sqrt{6}-2}$ is purely periodic.

Theorem 5.6 (Lagrange)**.** If $\theta \in \mathbb{R} \setminus \mathbb{Q}$, then continued fraction expansion of θ is essentially periodic $\iff$ θ is a quadratic irrational.

Proof.

$\Rightarrow$ If $\theta = [\overline{a_0, \dots, a_{k-1}}]$ is purely periodic, then

$$\theta = [a_0, \dots, a_{k-1}, \theta] \implies \theta = \frac{p_{k-1}\theta + p_{k-2}\theta}{q_{k-1}\theta + q_{k-2}}$$

Rearrange: get a quadratic equation satisfied by θ.

If $\theta = [a_0, \dots, a_{m-1}, \overline{a_m, \dots, a_{m+k-1}}]$ is essentially periodic, then $\theta = [a_0, \dots, a_{m-1}, \beta]$, where β has a purely periodic continued fraction expansion, so $\beta = r + s\sqrt{d}$. Now:

$$\theta = \frac{p_{m-1}\beta + p_{m-2}}{q_{m-1}\beta + q_{m-2}}$$

Rearrange to see θ has the form $r' + s'\sqrt{d}$, hence θ is a quadratic irrational.

$\Leftarrow$ Now suppose θ is a quadratic irrational, with continued fraction expansion $[a_0, a_1, a_2, \dots]$.a We know θ satisfies an equation $a\theta^2 + b\theta + c = 0$, $a, b, c \in \mathbb{Z}$. We define

$$f(x, y) = ax^2 + bxy + cy^2,$$

a BQF, with $f(0, 1) = 0$. For $n \geq 1$, define

$$f_n(x, y) = f\left(\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix}\right) = f(p_n x + p_{n-1} y, q_n x + q_{n-1} y).$$

Claim: As n varies, the sequence $f_n(x, y)$ takes on finitely many distinct BQFs. This implies the Theorem: For all $n \geq 1$,

$$\theta = [a_0, \dots, a_n, \theta_{n+1}] = \frac{\theta_{n+1} p_n + p_{n-1}}{\theta_{n+1} q_n + q_{n-1}}.$$

So

$$\begin{aligned} f_n(\theta_{n+1}, 1) &= f(p_n \theta_{n+1} + p_{n-1}, q_n \theta_{n+1} + q_{n-1}) \\ &= (q_n \theta_{n-1} + q_{n-1})^2 f\left(\frac{p_n \theta_{n+2} + p_{n-2}}{q_n \theta_{n+2} + q_{n-2}}, 1\right) \\ &= (q_n \theta_{n+1} + q_{n-1})^2 f(\theta, 1) \\ &= 0 \end{aligned}$$

Claim shows that as n varies, θ_{n+1} can take on only finitely many distinct values. Hence, there exist $n, k \geq 1$ such that $\theta_n = \theta_{n+k}$, hence continued fraction expansion of θ is essentially periodic.

Now we prove the claim: write $f_n(x, y) = A_n x^2 + B_n xy + C_n y^2$.

$$\begin{aligned} A_n &= f_n(1, 0) = f(p_n, q_n) \\ C_n &= f_n(0, 1) = f(p_{n-1}, q_{n-1}) = A_{n-1} \end{aligned}$$

So

$$\operatorname{disc} f_n = B_n^2 - 4A_n C_n = \operatorname{disc} f \cdot \det \begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix}^2 = \operatorname{disc} f$$

(as $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$). To show that claim, it's enough to show $|A_n|$ is bounded as n varies. Let's write θ' for the other root of $ax^2 + bx + c = 0$, so $f(x, 1) = a(x - \theta)(x - \theta')$. Then

$$|A_n| = |f(p_n, q_n)| = q_n^2 \left| f\left(\frac{p_n}{q_n}, 1\right) \right| = q_n^2 |a| \left| \frac{p_n}{q_n} - \theta \right| \left| \frac{p_n}{q_n} - \theta' \right|.$$

We know $\left|\theta - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n q_{n+1}}$ (proved last time). So

$$|A_n| \leq \frac{q_n^2}{q_n q_{n+1}} |a| \left| \frac{p_n}{q_n} - \theta' \right| \leq |a| \left| \frac{p_n}{q_n} - \theta' \right|.$$

We know $\left|\frac{p_n}{q_n} - \theta'\right| \to |\theta - \theta'|$ as $n \to \infty$. Therefore $|a| \left|\frac{p_n}{q_n} - \theta'\right|$ is bounded as n varies. $\square$

Theorem 5.7 (Galois)**.** Let $\theta = r + s\sqrt{d}$ be a quadratic irrational. Let $\theta' = r - s\sqrt{d}$ ("the other root of the quadratic"). Then the continued fraction expansion of θ is purely periodic $\iff$ $\theta > 1$, $\theta' \in (-1, 0)$.

In this case, if $\theta = [\overline{a_0, \dots, a_n}]$, then $-\frac{1}{\theta'} = [\overline{a_n, \dots, a_0}]$.

Proof. Omitted. ☐

Application: $\theta = \sqrt{d}$, $d \in \mathbb{Z}$ a non-square. Then $a_0 = \left\lfloor \sqrt{d} \right\rfloor$, $\theta_1 = \frac{1}{\sqrt{d} - a_0} > 1$.

$$\theta_1' = \frac{1}{-(\sqrt{d} + a_0)} \in (-1, 0)$$

Hence θ_1 satisfies hypothesis of Theorem 5.7. Hence

$$\sqrt{d} = [a_0, \overline{a_1, \dots, a_n}],$$

for some $n \geq 1$.

Theorem 5.8. Let $d \in \mathbb{N}$ be a non-square. Then the equation $X^2 - dY^2 = 1$ has a solution with $X, Y \in \mathbb{N}$.

Proof. Let $\sqrt{d} = [a_0, \overline{a_1, \dots, a_n}] = [a_0, \theta_1]$, $\theta_1 = [\overline{a_1, \dots, a_n}]$ (using the application of Theorem 5.7 above). Then

$$\sqrt{d} = [a_0, a_1, \dots, a_n, \overline{a_1, \dots, a_n}] = [a_0, \dots, a_n, \theta_1] = \frac{p_n \theta_1 + p_{n-1}}{q_n \theta_1 + q_{n-1}}$$

where $\theta_1 = \frac{1}{\sqrt{d} - a_0}$. Hence

$$\begin{aligned} \sqrt{d} &= \frac{p_n + p_{n-1}(\sqrt{d} - a_0)}{q_n + q_{n-1}(\sqrt{d} - a_0)} \\ \implies dq_{n-1} + (q_n - a_0 q_{n-1})\sqrt{d} &= (p_n - p_{n-1}a_0) + p_{n-1}\sqrt{d} \end{aligned}$$

Equate $\sqrt{d}$ and rational parts: $dq_{n-1} = p_n - p_{n-1}a_0$, $p_{n-1} = q_n - a_0 q_{n-1}$.

$p_{n-1}^2 - dq_{n-1}^2 = p_{n-1}(q_n - a_0 q_{n-1}) - p_n q_{n-1} + p_{n-1} q_{n-1} a_0 = p_{n-1} q_n - q_n q_{n-1} = (-1)^n$.

If n is even, then $p_{n-1}^2 - dq_{n-1}^2 = 1$, and we've found a solution. If n is odd, we run the same argument using

$$\sqrt{d} = [a_0, \overline{a_1, \dots, a_n, a_1, \dots, a_n}].$$ ☐

Start of lecture 21

Method to find solutions to Pell's equation $X^2 - dY^2 = 1$:

Compute the continued fraction expansion of $\sqrt{d}$ as

$$\sqrt{d} = [a_0, \overline{a_1, \dots, a_n}].$$

Look at $\frac{p_{n-1}}{q_{n-1}}$, the $(n-1)$-th convergent of $\sqrt{d}$. If n is even, then $p_{n-1}^2 - dq_{n-1}^2 = 1$. If n is odd, then $p_{n-1}^2 - dq_{n-1}^2 = -1$, but p_{2n-1}, q_{2n-1} will give a solution.

Example. $d = 6$, $\sqrt{d} = [2, \overline{2, 4}]$. $n = 2$, $\frac{p_1}{q_1} = 2 + \frac{1}{2} = \frac{5}{2}$. $5^2 - 6 \cdot 2^2 = 25 - 24 = 1$.

$d = 17$, $4 < \sqrt{17} < 5$, $a_0 = 4$, $\theta_1 = \frac{1}{\sqrt{17}-4} = \frac{\sqrt{17}+4}{17-16} = (\sqrt{17} - 4) + 8$. Then $a_1 = 8$, $\theta_2 = \frac{1}{\sqrt{17}-4} = \theta_1$, so $\sqrt{17} = [4, \overline{8}]$. So $n = 1$, $\frac{p_0}{q_0} = \frac{4}{1}$, $4^2 - 17 \cdot 1^2 = -1$. $\frac{p_1}{q_1} = 4 + \frac{1}{8} = \frac{33}{8}$. Then $33^2 - 17 \cdot 8^2 = 1$.

Remark. The solutions $(x, y) \in \mathbb{Z}^2$ to $x^2 - dy^2 = \pm 1$ correspond to *units* in the ring of integers in $\mathbb{Q}(\sqrt{d})$ ($\to$ Number Fields), via the formula

$$(x, y) \leftrightarrow x + \sqrt{d}y.$$

You can show that the solutions (x, y) to $x^2 - dy^2 = \pm 1$ are precisely the pairs $\pm(p_{kn-1}, q_{kn-1})$, where $k \geq 0$, and n is minimal such that $\sqrt{d} = [a_0, \overline{a_1, \dots, a_n}]$ (if $k = 0$, then $(p_{-1}, q_{-1}) = (1, 0)$ gives the trivial solution).

6 Primality testing and factorisation

Want to find processes to:

- Test whether a given integer $N \in \mathbb{N}$ is prime,
- If N is not prime, find a non-trivial factor.

Hope to do these in polynomial-time.

Can test primality in polynomial-time. Don't know how to factorise in polynomial-time, but there are algorithms that are much faster than trial division.

We'll usually assume $N > 1$ and that N is odd. (Can always divide by powres of 2 if N is even).

Begin by looking at necessary conditions for N to be prime. For example:

Example. If N is prime, $a \in \mathbb{Z}$, $(a, N) = 1$, then $a^{N-1} \equiv 1 \pmod{N}$ (Fermat's Little Theorem).

For example, if $N = 15$, $a = 2$, then $(a, N) = 1$, but

$$a^{N-1} = 2^{14} = (2^4)^3 2^2 \equiv 4 \not\equiv 1 \pmod{15}$$

Remark (Binary exponentiation)**.** Suppose $a, x, N \in \mathbb{N}$. Then we can compute $a^x \bmod N$ in polynomial-time. Write

$$x = \sum_{i=0}^{k} b_i 2^i, \qquad b_i \in \{0, 1\}.$$

Compute $a, a^2, a^4 = (a^2)^2, \dots, a^{2^k} = (a^{2^{k-1}})^2$. Then

$$a^x = \prod_{i=0}^{k} (a^{2^i})^{b_i}.$$

Example. $N = 91$, $a = 3$. Then $3^{90} = 3^{N-1} \equiv 1 \pmod{91}$. However, $N = 7 \times 13$ is composite.

Definition 6.1 (Fermat pseudoprime)**.** Let $N \in \mathbb{N}$ be an odd composite integer, $b \in \mathbb{Z}$, $(b, N) = 1$. We say N is a *Fermat pseudoprime to the base* b if $b^{N-1} \equiv 1 \pmod{N}$.

Remark. For fixed N, the condition of N being a Fermat pseudoprime to the base b only depends on $b \mod N$. So it makes sense for $b \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Proposition 6.2. Let $N \in \mathbb{N}$ be odd, composite. Then

(1) $\{b \in (\mathbb{Z}/N\mathbb{Z})^\times \mid N \text{ is a Fermat pseudoprime to the base } b\}$ is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$.

(2) If $\exists\, b_0 \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that N is not a Fermat pseudoprime to the base b_0 then the same is true for at least half of all $b \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Proof.

(1) Call this set H. We need to show $1 \in H$, and H closed under multiplication (since $(\mathbb{Z}/N\mathbb{Z})^\times$ is finite). $1^{N-1} \equiv 1 \pmod{N}$, so $1 \in H$.

If $b_1, b_2 \in H$, then $b_1^{N-1} \equiv 1 \equiv b_2^{N-1} \pmod{N}$. So $(b_1 b_2)^{N-1} \equiv b_1^{N-1} b_2^{N-1} \equiv 1 \pmod{N}$. So $b_1 b_2 \in H$.

(2) b_0 exists implies $H \neq (\mathbb{Z}/N\mathbb{Z})^\times$. We need to show $\#((\mathbb{Z}/N\mathbb{Z})^\times \setminus H) \geq \frac{\#(\mathbb{Z}/N\mathbb{Z})^\times}{2}$. We know $\#(\mathbb{Z}/N\mathbb{Z})^\times = \#H \cdot [(\mathbb{Z}/N\mathbb{Z})^\times : H] \geq 2\#H$. □

Idea for primality test: choose $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ at random and testing whether N is a Fermat pseudoprime to the base b.

Definition 6.3 (Carmichael number)**.** Let $N \in \mathbb{N}$ be odd and composite. We say N is a *Carmichael number* if it's a Fermat pseudoprime to every base $b \in (\mathbb{Z}/N\mathbb{Z})^\times$.

There exist infinitely many Carmichael numbers.

Definition 6.4 (Euler pseudoprime)**.** Let $N \in \mathbb{N}$ be odd and composite. Let $b \in \mathbb{Z}$ with $(b, N) = 1$. Then we say that N is an *Euler pseudoprime to the base* b if

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

Recall: If p is an odd prime, $(b, p) = 1$, then $b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod{p}$ (Euler's Criterion).

Remark. If $N$is an Euler pseudoprime to the base b, then it's a Fermat pseudoprime to the base b. This definition makes sense for $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, and it's again the case that

$$\{b \in (\mathbb{Z}/N\mathbb{Z})^\times \mid N \text{ is an Euler pseudoprime to the base } b\}$$

is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$.

Theorem 6.5. Let $N \in \mathbb{N}$ be odd, composite. Then there exists $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that N is not an Euler pseudoprime to the base b.

Proof. First assume N is squarefree, $N = pN_0$, p prime, $N_0 \ge 3$, $p \nmid N_0$. Since p is odd, there exists $u \in \mathbb{Z}$ such that $\left(\frac{u}{p}\right) = -1$. Choose $b \in \mathbb{Z}$ such that $b \equiv u \pmod{p}$, $b \equiv 1 \pmod{N_0}$ (using Chinese Remainder Theorem). Then

$$\left(\frac{b}{N}\right) = \left(\frac{b}{p}\right)\left(\frac{b}{N_0}\right) = \left(\frac{u}{p}\right)\left(\frac{1}{N_0}\right) = -1.$$

We know

$$b^{\frac{N-1}{2}} \equiv 1^{\frac{N-1}{2}} \equiv 1 \not\equiv -1 \pmod{N_0}.$$

So $b^{\frac{N-1}{2}} \not\equiv \left(\frac{b}{N}\right) \pmod{N}$. So b works.

Next suppose N is not squarefree, and choose p prime such that $p^2 \mid N$. Choose $b \in \mathbb{Z}$ such that $b \equiv 1 + p \pmod{p^2}$, $(b, N) = 1$ (Chinese Remainder Theorem). Then

$$b^{N-1} \equiv (1 + p)^{N-1} \equiv 1 + (N-1)p \equiv 1 - p \not\equiv 1 \pmod{p^2}.$$

So $b^{N-1} \not\equiv 1 \pmod{N}$, so N is not a Fermat pseudoprime to the base b, so certainly not an Euler pseudoprime to the base b. □

Start of

lecture 22

By Theorem 6.5, we deduce that

$$\{b \in (\mathbb{Z}/N\mathbb{Z})^\times \mid N \text{ is an Euler pseudoprime to the base } b\}$$

is a proper subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$. In particular, its complement contains at least half of the $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ (by the same argument as in Proposition 6.2).

This all forms the basis for the Soloray-Strassen probabilistic primality test:

Steps:

(0) Start with $N \in \mathbb{N}$ odd, $N > 1$.

(1) Choose b at random with $1 < b < N$. Test $(b, N) = 1$. If not, then N is composite, and stop.

(2) Otherwise, test if $b^{\frac{N-1}{2}} \equiv \left(\frac{b}{N}\right) \pmod{N}$. (Compute LHS by repeated squaring, RHS using Quadratic Reciprocity for Jacobi symbols). If not, then N is composite.

(3) If $b^{\frac{N-1}{2}} \equiv \left(\frac{b}{N}\right) \pmod{N}$, then either N is prime, or N is an Euler pseudoprime to the base b.

If we get to Step 3, then N is composite with probability $\leq \frac{1}{2}$. If we carry out the whole procedure $k \geq 1$ times, then either we will prove that N is composite, or we will know that N is prime with probability $\geq 1 - \frac{1}{2^k}$.

We can refine this further.

Suppose p is an odd prime, $a \in \mathbb{Z}$, $(a, p) = 1$. Then $a^{p-1} \equiv 1 \pmod{p}$, hence $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ (as p is prime).

If $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and $4 \mid p - 1$, then $a^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}$.

If $a^{\frac{p-1}{4}} \equiv 1 \pmod{p}$ and $8 \mid p - 1$, then $a^{\frac{p-1}{8}} \equiv \pm 1 \pmod{p}$.

Definition 6.6 (Strong test)**.** Let $N \in \mathbb{N}$, odd, $N > 1$. Factor $N - 1 = 2^s t$, t odd, $s \geq 1$. Let $b \in \mathbb{Z}$, $(b, N) = 1$. Then we say N passes the *strong test* to the base b if either $b^t \equiv 1 \pmod{N}$ or if $b^{2^r t} \equiv -1 \pmod{N}$ for some $0 \leq r < s$.

If N is composite and passes the strong test to the base b, then we say that N is a *strong pseudoprime* to the base b.

Example. $N = 65$, $b = 8$. Then $N - 1 = 2^6$. Need to test whether: $b^1 \equiv 1 \pmod p$ or $b^{2^i} \equiv -1 \pmod p$ for some $0 \le i < 6$.

$8 \not\equiv 1 \pmod{65}$, but $8^2 \equiv -1 \pmod{65}$. Therefore 65 is a strong pseudoprime to the base 8.

Now take $N = 65$, $b = 2$. Need to test whether: $2 \equiv 1 \pmod N$ or if $2^{2^i} \equiv -1 \pmod N$ for some $0 \le i < 6$.

$$\begin{aligned} 2 &\not\equiv \pm 1 \pmod N \\ 2^2 &= 4 \not\equiv -1 \pmod N \\ 2^{2^2} &= 16 \not\equiv -1 \pmod N \\ 2^{2^3} &= 16^2 = 4 \times 8^2 \equiv -4 \not\equiv -1 \pmod N \\ 2^{2^4} &= (-4)^2 \equiv 16 \not\equiv -1 \pmod N \\ 2^{2^5} &= (16)^2 \equiv 4 \not\equiv -1 \pmod N \end{aligned}$$

Hence 65 does not pass the strong test to the base 2.

Remark. If N is a strong pseudoprime to the base b, then it's also an Euler pseudoprime to the base b.

You can show that if $N \in \mathbb{N}$ is odd and composite, then it's a strong pseudoprime to at most $\frac{1}{4}$ of bases $b \in (\mathbb{Z}/N\mathbb{Z})^\times$. This leads to the Miller-Rabin probabilistic primality test.

(1) Choose $1 < b < N$ at random, and test if $(b, N) = 1$.

(2) If $(b, N) = 1$, test to see if N passes the strong test to the base b.

(3) If it doesn't pass, then N is composite. If it does pass, then N is composite with probability $\le \frac{1}{4}$.

If we assume the generalised Riemann hypothesis, then we can use the strong test to get a deterministic polynomial-time primality test.

Theorem 6.7. Assume Generalised Riemann Hypothesis. Let $N \in \mathbb{N}$ be odd and composite. Then there exists $b \in \mathbb{N}$, $b < 2(\log N)^2$, such that N is not a strong pseudoprime to the base b.

So, assuming Generalised Riemann Hypothesis, can prove N is prime / composite by carrying out strong test for all $b < 2(\log N)^2$.

There is an unconditional (not assuming any unproved conjectures) polynomial-time primality test: the Agrawal-Kayal-Saxena test. This is harder to implement than the strong test.

We now discuss factorisation. Suppose $N \in \mathbb{N}$ is odd and composite. Say $N = ab$, $a > b > 1$. Then $N = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$.

Conversely, if $N = r^2 - s^2$, where $r, s \in \mathbb{N}$, $r > s + 1$, then $N = (r+s)(r-s)$ is a non-trivial factorisation.

This leads to Fermat factorisation: Assume N is not a perfect square.

Then test each of $r = \lfloor\sqrt{N}\rfloor + 1, \lfloor\sqrt{N}\rfloor + 2, \lfloor\sqrt{N}\rfloor + 3, \dots$ to see if $r^2 - N$ is a perfect square, say $r^2 - N = s^2$, $s \in \mathbb{N}$.

If $r = \frac{a+b}{2}$, then $r > \sqrt{ab} = \sqrt{N}$. So this will find the factorisation $N = ab$, and after at most $\frac{a-b}{2}$ steps. This is useful if we know that $N = ab$ has a factorisation where $|a - b|$ is small.

Example. $N = 200819$. $\lfloor\sqrt{200819}\rfloor = 448$. $449^2 - N = 782$ (not a square). But $450^2 = 1681 = 41^2$. So $N = 200819 = (450+41)(450-41) = 491 \times 409$.

Start of lecture 23

Proposition 6.8. Let $N \in \mathbb{N}$ be odd and composite. Suppose $\exists r, s \in \mathbb{Z}$ such that $r \not\equiv \pm s \pmod{N}$, but $r^2 \equiv s^2 \pmod{N}$. Then $(N, r+s)$ and $(N, r-s)$ are non-trivial factors of N.

Proof. By hypothesis, $r^2 \equiv s^2 \pmod{N} \implies (r+s)(r-s) \equiv 0 \pmod{N}$. Let's show $(N, r-s)$ is a non-trivial factor of N (other case is similar). $(N, r-s) \mid N$, so we need to show that $(N, r-s) \notin \{1, N\}$. If $(N, r-s) = N$, then $N \mid r - s$ so $r \equiv s \pmod{N}$ ※. If $(N, r-s) = 1$, then $r - s \pmod{N}$ has a multiplicative inverse, hence $r + s \equiv 0 \pmod{N}$, so $r \equiv -s \pmod{N}$ ※. □

Directly finding r, s as in the Proposition is tricky. Indeed, we look for integers x_i such that $x_i^2 = c_i \pmod{N}$ for some c_i such that the c_i have a "small" number of prime factors as i varies.

Lemma 6.9. Let $p_1, \dots, p_r$ be distinct primes, and let $c_1, \dots, c_k$ be non-zero integers divisible only by primes in $\{p_1, \dots, p_r\}$. Then if $k > r+1$, then there exists a non-empty subset $J \subset \{1, \dots, k\}$ such that

$$c_J = \prod_{j \in J} c_j$$

is a square.

Proof. Pigeonhole principle: for any $J \subset \{1, \dots, k\}$, let $c_J = \prod_{j \in J} c_j$. Write

$$c_J = (-1)^{\alpha_{J,0}} \left(\prod_{i=1}^{r} p_i^{\alpha_{J,i}} \right) b_J^2$$

where $b_J \in \mathbb{N}$, $\alpha_{J,i} \in \{0,1\}$, $i = 0, \dots, r$. There are 2^k choices for a subset $J \subset \{1, \dots, k\}$, and 2^{r+1} possibilities for $\alpha_J = (\alpha_{J,0}, \dots, \alpha_{J,r})$. If $k > r+1$, then there exist $J, J' \subset \{1, \dots, k\}$ with $J \neq J'$ such that $\alpha_J = \alpha_{J'}$. Then

$$c_J c_{J'} = \left((-1)^{\alpha_{J,0}} \prod_{i=1}^{r} p_i^{\alpha_{J,i}} \right) b_J^2 b_{J'}^2$$

is a square. Also,

$$c_J c_{J'} = \left(\prod_{j \in J} c_j \right) \left(\prod_{j \in J'} c_j \right) c_{(J \triangle J')} (c_{(J \cap J')})^2,$$

where $J \triangle J' = (J \cup J') \setminus (J \cap J')$ (which is non-empty since $J \neq J'$). We see that $c_{J \triangle J'}$ is a square. □

Definition 6.10 (Factor base)**.** Let $N \in \mathbb{N}$ be an odd composite integer. A *factor base* is a set $B = \{-1, p_1, \dots, p_r\}$ 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, where $\langle x^2 \rangle$ is the unique integer such that $\langle x^2 \rangle \equiv x^2 \pmod{N}$ and $-\frac{N}{2} < \langle x^2 \rangle < \frac{N}{2}$.

We now describe the factor base method to factorise an odd composite $N \in \mathbb{N}$.

Step 1 Choose a factor base B.

Step 2 Generate some B-numbers $x_1, \dots, x_k$.

Step 3 Find a non-empty subset $J \subset \{1, \dots, k\}$ such that $\prod_{j \in J} \langle x_j^2 \rangle = y^2$, some $y \in \mathbb{N}$. Then if $x = \prod_{j \in J} x_j$, then $x^2 \equiv y^2 \pmod{N}$. If $x \not\equiv \pm y \pmod{N}$, then by Proposition 6.8, $(N, x+y)$, $(N, x-y)$ are non-trivial factors of N. If $x \equiv \pm y \pmod{N}$, then go back to Step 2 and try again.

This is only a method, not an algorithm. When can this method work? If we find x, y and $(x, N) = (y, N) = 1$, then $\frac{x}{y} \pmod{N}$ is a solution to $x^2 \equiv 1 \pmod{N}$, which we want not to equal $\pm 1 \pmod{N}$.

If $N = \prod_{i=1}^{s} p_i^{e_i}$, p_i distinct primes, $e_i \geq 1$. Then

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong \prod_{i=1}^{s} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times.$$

So there are 2^s solutions to $x^2 \equiv 1 \pmod{N}$. If $s \geq 2$, then we can expect $\frac{x}{y} \not\equiv \pm 1 \pmod{N}$ with probability $\frac{2^s - 2}{2^s} = 1 - 2^{1-s} > 0$. If $s = 1$, then the method witll never give a factorisation.

This is OK, as we can test whether $N = m^k$ for some $k \geq 2$ in polynomial time. For each $2 \leq k \leq \frac{\log N}{\log 3}$, let x be the closest integer to $\sqrt[k]{N}$ and test to see if $N = x^k$.

One way to generate B-numbers: consider x of the form $\left\lfloor \sqrt{kN} \right\rfloor$, $\left\lfloor \sqrt{kN} \right\rfloor + 1$, for $k = 1, 2, \dots$. Then x^2 should be "close" to a multiple of N, so $\langle x^2 \rangle$ should be "close" to 0 so should have only small prime factors.

Example. $N = 1829$, $B = \{-1, 2, 3, 5, 7, 11, 13\}$. Calculate $\left\lfloor\sqrt{k1829}\right\rfloor = 42, 60, 74, 85$ for $k = 1, 2, 3, 4$.

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

We find

$$\begin{aligned}(42 \times 43 \times 61 \times 85)^2 &\equiv \langle 42^2 \rangle \times \langle 43^3 \rangle \times \langle 61^2 \rangle \times \langle 85^2 \rangle \pmod{1829} \\ &= (-5 \times 13 \times 2^2 \times 5 \times 3^2 \times 7 \times -7 \times 13) \\ &= (2 \times 3 \times 5 \times 7 \times 13)^2\end{aligned}$$

$42 \times 43 \times 61 \times 85 \equiv 1459 \pmod{1829}$. $2 \times 3 \times 5 \times 7 \times 13 = 901$. Hence if $1459 \not\equiv \pm 901 \pmod{1829}$, then $(1829, 1459 \pm 901)$ are non-trivial factors of 1829. We find $(1829, 2360) = 59$, $(1829, 558) = 31$, $31 \times 59 = 1829$.

Remark. In this case, $N = (N, x + y)(N, x - y)$. This does not always happen.

Start of lecture 24

Remark (Remarks on implementation)**.**

(1) To decide if x is a B-number, we need to know if x is a product of numbers of B. We do this by trial division by numbers of B.

(2) We showed last time using the pigeonhole principle that if $k > r + 1$, then a non-trivial relation $\prod_{i \in I} \langle x_i^2 \rangle = y^2$ must exist. It's faster in practice to use linear algebra over $\mathbb{Z}/2\mathbb{Z}$.

Let's now discuss another way to generate B-numbers, using continued fractions.

Lemma 6.11. Let $N \in \mathbb{N}$ be odd, composite and not square. Let $\frac{p_n}{q_n}$ be a convergent of $\sqrt{N}$. Then $|p_n^2 - Nq_n^2| < 2\sqrt{N}$.

Why this is useful: it says $p_n^2 - Nq_n^2$ is close to 0, i.e. p_n^2 is close to a multiple of N, and p_n has a good chance of being a B-number.

Proof. We use $\left|\frac{p_n}{q_n} \le \frac{1}{q_n q_{n+1}}\right|$ (true for any $\theta \in \mathbb{R} \setminus \mathbb{Q}$). Then

$$|p_n^2 - Nq_n^2| = q_n^2 \left|\frac{p_n}{q_n} - \sqrt{N}\right| \left|\frac{p_n}{q_n} + \sqrt{N}\right| \le \frac{q_n^2}{q_n q_{n+1}} \left(2\sqrt{N} + \frac{1}{q_n q_{n+1}}\right)$$

RHS equals

$$\begin{aligned} \frac{1}{q_{n+1}} \left(2q_n\sqrt{N} + \frac{1}{q_{n+1}}\right) &\le \frac{\sqrt{N}}{q_{n+1}}(2q_n + 1) \\ &= 2\sqrt{N} \left(\frac{q_n + \frac{1}{2}}{q_{n+1}}\right) \\ &< 2\sqrt{N} \end{aligned}$$

as $q_{n+1} > q_n$. □

Note. We only care about $p_n \pmod N$. We can compute this using the recurrence relation $p_n = a_n p_{n-1} + p_{n-2} \pmod N$.

Example. $N = 12403$. Then $\sqrt{N} = [111, 2, 1, 2, 2, 7, 1, \dots]$.

$p_n \pmod N$	$\langle p_n^2 \rangle$	factorisation	B-number?
111	-82	-2×41	✗
223	117	$3^2 \times 13$	✓
334	-71	-71	✗
891	89	89	✗
2116	-27	3^3	✓
3300	166	2×83	✗
5416	-39	-3×13	✓

$B = \{-1, 3, 13\}$ (when calculating by hand, it is convenient to choose the factor base after calculating some potential B-numbers).

We see $\langle 223^2 \rangle \times \langle 2116^2 \rangle \times \langle 5416^2 \rangle = (3^2 \times 13)^2$. We compute $223 \times 2116 \times 5416 \equiv 11341 \pmod N$. $3^3 \times 13 \equiv 351 \pmod N$.

Then $(12403, 11341 \pm 351) = 157, 79$, which are non-trivial factors of N.

Generalisations of factor base method include the “quadratic sieve” and “ umber field sieve” – fastest factoring algorithm for very large N.

One can also develop methods to find prime factors of N of particular types. We give the example of the Pollard $(p-1)$-method, to find prime factors $p \mid N$ such that $p-1$ is divisible only by small primes.

Suppose $N \in \mathbb{N}$ is odd and composite, and $N = pN_0$ with $(p, N_0) = 1$. Suppose $a \in \mathbb{Z}$, $(a, N) = 1$. Then $a^{p-1} \equiv 1 \pmod p$ by Fermat's Little Theorem. We expect to have $q^{p-1} \not\equiv 1 \pmod{N_0}$, so we expect $(a^{p-1} - 1, N)$ to be a non-trivial factor of N. Computing $a^{p-1} \pmod N$ requires knowing p.

Pollard's $(p-1)$-method:

(1) Choose $m \geq 2$, let $k = \mathrm{lcm}(1, 2, \ldots, m)$.

(2) Choose $a \geq 2$, test $(a, N) = 1$. If not, we have found a non-trivial factor of N.

(3) Otherwise, compute $a^k \pmod N$ by repeated squaring, and hope $(N, a^k - 1)$ is a non-trivial factor of N.

This method should find those prime factors $p \mid N$ such that every prime power dividing $p-1$ is $\leq m$.

Reason: In this case, $p - 1 \mid k$, so $a^{p-1} \equiv 1 \pmod p$, hence $a^k \equiv 1 \pmod p$, so $p \mid (N, a^k - 1)$.

Example. $N = 540143$, $m = 8$, $k = \mathrm{lcm}(1, 2, \ldots, 8) = 840$.

$a = 2$: $840 = 8(64 + 32 + 8 + 1)$, so $2^k \equiv (2^{64+32+8+1})^8 \equiv 53047 \pmod N$. We compute $(540143, 53046) = 421$, a prime factor of N.

Note $421 - 1 = 2^2 \times 3 \times 5 \times 7$.

Note. There exists a polynomial-time algorithm to factorise integers (Shor's algorithm), which requires a scalable quantum computer.

Current research topic: find cryptosystems, implementable today, which will remain secure even if such computers become widely available.

Index