Number Theory

Lectured by V. Neale

Michaelmas Term 2011

NUMBER THEORY (C) **24 lectures, Michaelmas term**

Official course blog: http://theoremoftheweek.wordpress.com/category/lecture/

Note. Text in grey indicates an aside or comment made by the lecturer. (For those who attended the lectures, these were the comments in yellow chalk.)

Transcribed from a student's notes; please let me know of corrections: glt1000@cam.ac.uk
Last updated: Tue 5th Sept, 2017

Number Theory

Lecture 1

Definition. The **natural numbers** are $\mathbb{N} = \{1, 2, 3, \ldots\}$.

Definition. The non-negative integer a **divides** the integer b if there is an integer k such that $b = ka$. In this case we write $a \mid b$ (read as "a divides b"), and we also say that a is a **factor** or **divisor** of b and that b is **divisible** by a. If not, we write $a \nmid b$.

Definition. A natural number n greater than 1 is **prime** exactly when its only (positive) factors are 1 and n. If n has a non-trivial factor (that is, other than 1 and n) then n is **composite**. It is convenient to define 1 to be neither prime nor composite.

Definition. The **prime counting function** $\pi(x)$ counts the number of primes less than or equal to x. That is, $\pi(x) = \#\{p \leqslant x : p \text{ prime}\}$.

Lemma 1. Let n be a natural number greater than 1. Then n has a prime factor.

Proof. By induction on n. For $n = 2$, done.

Suppose true for $2, 3, \ldots, n-1$, and consider n. If n is prime then done. If n is composite then n has a factor $a \in \{2, 3, \ldots, n-1\}$. By the induction hypothesis, a has a prime factor, say p. But then p is a prime factor of n. □

Theorem 2. There are infinitely many primes. (That is, $\pi(x) \to \infty$ as $x \to \infty$.)

Remark. We'll use Euclid's proof now. We'll return to the distribution of the primes later in the course.

Proof. By contradiction. Suppose there are finitely many primes, say $2, 3, 5, \ldots, p$.

Consider $N = 2 \times 3 \times 5 \times \cdots \times p + 1$. By Lemma 1, N has a prime factor. This prime factor can't be 2, or 2 would divide $N - 2 \times 3 \times 5 \times \cdots \times p = 1$. In the same way, it can't be $3, 5, \ldots, p$. ⨳ □

Remark. We don't care if N itself is prime.

Definition. The **highest common factor** (hcf) of the natural numbers a and b is the largest integer d such that $d \mid a$ and $d \mid b$. If may be written as $\text{hcf}(a, b)$ or (a, b). It is also called the **greatest common divisor** (gcd).

Examples. $\text{hcf}(6, 15) = 3$, $\text{hcf}(6, 18) = 6$.

Definition. If $\text{hcf}(a, b) = 1$, say that a and b are **coprime** (or **relatively prime**).

Euclid's algorithm. We find $\text{hcf}(117, 51)$.

$$
\begin{array}{rcrcrl}
117 & = & 2 \times 51 & + & 15 & \text{(put numbers doing same job in same place)} \\
51 & = & 3 \times 15 & + & 6 & \\
15 & = & 2 \times 6 & + & 3 & \longleftarrow \text{hcf is last non-zero remainder} \\
6 & = & 2 \times 3 & + & 0 &
\end{array}
$$

More generally, to find $\text{hcf}(a, b)$ where $a > b$:

$$\begin{array}{lrcll}
\text{Divide } a \text{ by } b: & a & = & q_1 \times b + r_1 & (0 \leqslant r_1 < b) \\
\text{Divide } b \text{ by } r_1: & b & = & q_2 \times r_1 + r_2 & (0 \leqslant r_2 < r_1) \\
& r_1 & = & q_3 \times r_2 + r_3 & \\
& & \vdots & & \\
& r_{k-2} & = & q_k \times r_{k-1} + r_k & (r_k \neq 0) \\
& r_{k-1} & = & q_{k+1} \times r_k + 0 &
\end{array}$$

Proposition 3. "Euclid's algorithm works."

Let a, b be natural numbers with $a > b$, and let q_i and r_j be obtained from Euclid's algorithm as above. Then there is some k (with $r_k \neq 0$) such that $r_{k-1} = q_{k+1} r_k$; that is, the algorithm terminates. Moreover, $r_k = \text{hcf}(a, b)$.

Proof.

(i) The remainders r_j form a strictly decreasing sequence of non-negative integers which must stop at 0.

(ii) First, we show $r_k \mid a$ and $r_k \mid b$ (i.e., it's a common factor).

From the last equation, $r_k \mid r_{k-1}$.

From the next up, $r_k \mid$ RHS, so $r_k \mid r_{k-2}$. Etc. So $r_k \mid r_1$, and $r_k \mid b$, $r_k \mid a$.

Now suppose $d \mid a$ and $d \mid b$. We want $d \mid r_k$.

From the top equation, $d \mid r_1$. From the second, $d \mid r_2$. Etc. So $d \mid r_k$. □

Theorem 4 (Bézout). Let a, b, c be natural numbers. There are integers m, n such that $am + bn = c$ if and only if $(a, b) \mid c$.

Proof. ($\Rightarrow$). Have integers m, n such that $am + bn = c$. But $(a, b) \mid a$ and $(a, b) \mid b$ by definition, so $(a, b) \mid c$.

Lecture 2

($\Leftarrow$). We want to show that if c is a multiple of (a, b) then it can be written as a linear combination of a and b. Start with special case $c = (a, b)$.

Run Euclid's algorithm on a, b (wlog $a \geqslant b$).

$$\begin{array}{rcl}
a & = & q_1 \times b + r_1 \\
b & = & q_2 \times r_1 + r_2 \\
r_1 & = & q_3 \times r_2 + r_3 \\
& \vdots & \\
r_{k-3} & = & q_{k-1} \times r_{k-2} + r_{k-1} \\
r_{k-2} & = & q_k \times r_{k-1} + r_k \\
r_{k-1} & = & q_{k+1} \times r_k + 0
\end{array}$$

We know that $r_k = (a, b)$

$$\begin{array}{rcl}
& = & r_{k-2} - q_k r_{k-1} \\
& = & r_{k-2} - q_k (r_{k-3} - q_{k-1} r_{k-2}) \\
& = & \ldots \text{ (continue substituting)} \\
& = & am + bn \text{ for some } m, n \in \mathbb{Z}
\end{array}$$

If $c = (a, b)c'$ then $c = a(mc') + b(nc')$ is of the required form. □

Example. We want m, n such that $117m + 51n = 3$.

$$\begin{array}{rcl} \text{By Euclid, } 3 &=& 15 - 2 \times 6 \\ &=& 15 - 2 \times (51 - 3 \times 15) \qquad = \quad 7 \times 15 - 2 \times 51 \\ &=& 7 \times (117 - 2 \times 51) - 2 \times 51 \quad = \quad 7 \times 117 - 16 \times 51 \end{array}$$

I.e., take $m = 7$, $n = -16$.

Exercise. Find all solutions to $117m + 51n = 3$.

Proposition 5. Let p be a prime. If p divides the product ab, then $p \mid a$ or $p \mid b$.

(In fact, one could use this property to *define* prime numbers – see *Number Fields*.)

Proof. (Avoid prime factorisations.)

Assume $p \mid ab$ and $p \nmid a$. We aim to show that $p \mid b$. Since $p \nmid a$ and p is prime, we have $(a, p) = 1$. So by Bézout, there are integers m, n such that $am + pn = 1$.

Then $\underset{\substack{\uparrow \\ p|ab}}{abm} + \underset{\substack{\uparrow \\ p|p}}{pbn} = b$. So $p \mid$ LHS, so $p \mid$ RHS, so $p \mid b$. □

Remark. This is a good illustration of the use of Bézout.

Theorem 6 (Fundamental Theorem of Arithmetic). Let n be a natural number. Then n can be factorised as a product of primes in an essentially unique way (i.e., up to ordering).

(This treats the factorisation of 1 as the "empty product" – or leave out.)

Proof. Existence. By induction on n. (Exercise: see Lemma 1.)

Uniqueness. Suppose that $n = p_1 \ldots p_k = q_1 \ldots q_\ell$, where p_i, q_j are primes.

Then $q_1 \mid p_1 \ldots p_k$, so by Proposition 5, $q_1 \mid p_i$ for some i. But p_i is prime, so $q_1 = p_i$.

Now cancel and repeat. Get $k = \ell$, and $p_1, \ldots, p_k$ and $q_1, \ldots, q_\ell$ are the same lists. □

Definition. We say that a is **congruent to** b **modulo** n, written $a \equiv b \pmod{n}$, exactly when n divides $b - a$.

More abstract: $\mathbb{Z}$ is a commutative ring and $n\mathbb{Z} = \{nm : m \in \mathbb{Z}\}$ is an ideal; the cosets of $n\mathbb{Z}$ are the congruence classes coming from the equivalence relation $\equiv$.

E.g., $[3]_7 = \{\ldots, -11, -4, 3, 10, 17, \ldots\} = 3 + 7\mathbb{Z}$.

We're interested in the quotient ring $\mathbb{Z}/n\mathbb{Z}$.

We define $[a]_n + [b]_n = [a + b]_n$ and $[a]_n[b]_n = [ab]_n$.

(Exercise: check these are well-defined, and that we get the ring $\mathbb{Z}/n\mathbb{Z}$.)

Lemma 7. Let n be a natural number greater than 1 and let a be an integer coprime to n. Then a has a multiplicative inverse mod n, i.e. there exists m such that $am \equiv 1 \pmod{n}$.

Proof. Since $(a, n) = 1$, there are integers ℓ and m such that $am + n\ell = 1$, and then $am \equiv 1 \pmod{n}$. □

Exercise. If $(a, n) > 1$ then a does not have a multiplicative inverse modulo n.

Remark. If p is prime then $\mathbb{Z}/p\mathbb{Z}$ is a field.

Definition. The **multiplicative group** modulo n, written $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ or $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$, is the group of invertible elements (or **units**) modulo n.

We write $\phi(n)$ (or $\varphi(n)$) for $\left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right|$ – this is the **Euler totient function**.

Examples. If p is prime then $\phi(p) = \left|\left(\mathbb{Z}/p\mathbb{Z}\right)^\times\right| = p - 1$. And $\phi(8) = 4$.

Remark. By Lemma 7, we have $\phi(n) = \#\{a : 1 \leqslant a \leqslant n \text{ and } (a, n) = 1\}$.

Theorem 8 (Fermat-Euler). Let n be a natural number greater than 1, and let a be an integer coprime to n.

Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Remark. If $n = p$, prime, we get Fermat's Little Theorem: $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Apply Lagrange's Theorem to the group $G = \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$. We have $a \in G$, so its order divides $|G| = \phi(n)$. I.e., $a^{|G|} = a^{\phi(n)} \equiv 1 \pmod{n}$. □

Lecture 3

We are interested in simultaneous linear congruences, such as

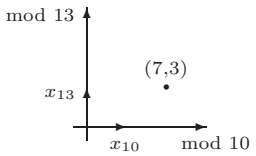
$$\begin{array}{lll} (1) & n \equiv 7 & \pmod{10} \\ & n \equiv 3 & \pmod{15} \end{array} \qquad \text{or} \qquad \begin{array}{lll} (2) & n \equiv 7 & \pmod{10} \\ & n \equiv 3 & \pmod{13} \end{array}$$

In (1), $\left.\begin{array}{l} n \equiv 7 \pmod{10} \implies n \equiv 2 \pmod{5} \\ n \equiv 3 \pmod{15} \implies n \equiv 3 \pmod{5} \end{array}\right\}$ mutually incompatible, so no solutions.

The problem was that $(10, 15) > 1$.

(2). Suppose we had x_{10}, x_{13} such that

$$\begin{array}{rlrl} x_{10} \equiv 1 & \mod 10, & x_{13} \equiv 1 & \mod 13 \\ \equiv 0 & \mod 13, & \equiv 0 & \mod 10 \end{array}$$



Then we can in fact make any point by a suitable linear combination. E.g., $n = 7x_{10} + 3x_{13}$ for our example.

But we can find such x_{10} and x_{13}. Since $(10, 13) = 1$, Bézout tells us that there exist h, k such that $\underbrace{10h}_{x_{13}} + \underbrace{13k}_{x_{10}} = 1$.

And Euclid's algorithm means we can find h and k.

Theorem 9 (Chinese Remainder Theorem). Let m_1, m_2 be coprime natural numbers greater than 1, and let a_1, a_2 be integers. Then there is a solution n to the simultaneous congruences

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \end{aligned}$$

and moreover this solution is unique modulo $m_1 m_2$.

Proof. (Existence). Since $(m_1, m_2) = 1$, Bézout gives integers h, k such that $m_1 h + m_2 k = 1$.

Let $x_1 = m_2 k$ and $x_2 = m_1 h$. $\left(\begin{array}{lll} \text{So} & x_1 \equiv 1 \pmod{m_1} & \text{and} \quad x_2 \equiv 0 \pmod{m_1} \\ & x_1 \equiv 0 \pmod{m_2} & \qquad\quad x_2 \equiv 1 \pmod{m_2} \end{array}.\right)$

Then $n = a_1 x_1 + a_2 x_2$ is a solution.

(Uniqueness). Suppose n and n' are solutions. Then $\begin{aligned} n \equiv a_1 \equiv n' \pmod{m_1} \\ n \equiv a_2 \equiv n' \pmod{m_2} \end{aligned}$

So $m_1 \mid n - n'$ and $m_2 \mid n - n'$.

Since $(m_1, m_2) = 1$, this gives $m_1 m_2 \mid n - n'$. That is, $n \equiv n' \pmod{m_1 m_2}$. □

Remarks.

1. It is not difficult to extend to systems of more congruences, as long as the moduli are *pairwise coprime* (i.e., $(m_i, m_j) = 1$ if $i \neq j$).
2. If the moduli are not pairwise coprime, then there may or may not be a solution.
3. We can phrase this more algebraically: the map

$$\begin{array}{ccc} \mathbb{Z}/m_1 m_2 \mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \\ n & \longmapsto & (n \bmod m_1, n \bmod m_2) \end{array}$$

is an isomorphism of rings. More generally, if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $p_1, \ldots, p_k$ are distinct primes and $\alpha_1, \ldots, \alpha_k \geqslant 1$, then

$$\mathbb{Z}/n\mathbb{Z} \;\cong\; \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$$

Slogan. "Work modulo powers of primes and then piece together information".

Corollary. Let m_1, m_2 be as above and let a_1, a_2 be integers with $(a_1, m_1) = 1$, $(a_2, m_2) = 1$. Then there is a solution to

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \end{aligned}$$

and any such solution is coprime to $m_1 m_2$.

Proof. Theorem 9 says that there is a solution. Suppose that $(n, m_1 m_2) > 1$. Then there is a prime p such that $p \mid n$ and $p \mid m_1 m_2$. Wlog $p \mid m_1$.

We have $n \equiv a_1 \pmod{m_1}$ so $p \mid a_1$. But then $(m_1, a_1) = p$. ⨳

So $(n, m_1 m_2) = 1$. □

We can phrase this more algebraically:

$$\left(\mathbb{Z}/m_1 m_2 \mathbb{Z}\right)^\times \;\cong\; \left(\mathbb{Z}/m_1\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/m_2\mathbb{Z}\right)^\times$$

More generally, if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then:

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \;\cong\; \left(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}\right)^\times$$

Definition. Let $f : \mathbb{N} \to \mathbb{N}$. We say that f is **multiplicative** if $f(mn) = f(m)f(n)$ whenever m and n are coprime.

We say that f is **totally multiplicative** if $f(mn) = f(m)f(n)$ for all m, n.

Corollary 11. The Euler ϕ function is multiplicative. (Define $\phi(1) = 1$.)

Remark. ϕ is *not* totally multiplicative. E.g., $\phi(4) = 2$, $\phi(2)\phi(2) = 1$.

Proof. Let m, n be coprime. Then

$$\phi(mn) \;=\; \left|\left(\mathbb{Z}/mn\mathbb{Z}\right)^\times\right| \;=\; \left|\left(\mathbb{Z}/m\mathbb{Z}\right)^\times\right| \times \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right| \;=\; \phi(m)\phi(n) \qquad \square$$

It follows that if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then $\phi(n) = \phi(p_1^{\alpha_1}) \cdots \phi(p_k^{\alpha_k})$.

Slogan. "Work with $\phi(p^k)$ and piece together".

Lemma 12. Let p be a prime and let k be a natural number. Then $\phi(p^k) = p^{k-1}(p-1)$.

Proof. We have $\phi(p^k) = \#\{a : 1 \leqslant a \leqslant p^k \text{ and } (a,p) = 1\}$. We have p^k values to consider, and we must discard multiples of p : i.e., p, $2p$, $3p$, $\ldots$, $p^{k-1}p$. There are p^{k-1} of these, so $\phi(p^k) = p^k - p^{k-1}$. $\square$

We are going to be interested in $\sum_{d|n} \phi(d)$. (Have n fixed and sum over divisors of n.)

Example.

$$\begin{aligned}
\sum_{d|12} \phi(d) &= \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) \\
&= \phi(1) + \phi(2) + \phi(3) + \phi(2^2) + \phi(2)\phi(3) + \phi(2^2)\phi(3) \\
&= \left[\phi(1) + \phi(2) + \phi(2^2)\right]\left[\phi(1) + \phi(3)\right] \\
&= \left(\sum_{d|4} \phi(d)\right)\left(\sum_{d|3} \phi(d)\right) \\
&= (1+1+2)(1+2) \;=\; 4 \times 3 \;=\; 12.
\end{aligned}$$

Lecture 4

Lemma 13. Let n be a natural number. Then $\sum_{d|n} \phi(d) = n$.

Proof. Let $F(n) = \sum_{d|n} \phi(d)$. Let m, n be coprime. Then

$$\begin{aligned}
F(mn) &= \sum_{d|mn} \phi(d) \\
&= \sum_{\substack{d_1|m \\ d_2|n}} \phi(d_1 d_2) \qquad \text{since } (m,n) = 1 \\
&= \left(\sum_{d_1|m} \phi(d_1)\right)\left(\sum_{d_2|n} \phi(d_2)\right) \qquad \text{as } (d_1, d_2) = 1, \text{ by Corollary 11} \\
&= F(m)F(n)
\end{aligned}$$

So F is multiplicative.

Let p be prime, and $j \geqslant 1$. Then

$$\begin{aligned} F(p^j) &= \sum_{i=0}^{j} \phi(p^i) \\ &= 1 + \sum_{i=1}^{j} (p^i - p^{i-1}) \quad \text{by Lemma 12} \\ &= 1 + (p-1) + (p^2 - p) + \cdots + (p^j - p^{j-1}) = p^j \end{aligned}$$

So if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where the p_i are distinct primes, then $F(n) = F(p_1^{\alpha_1}) \cdots F(p_k^{\alpha_k}) = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = n$. □

Remark. The proof that F is multiplicative used only the fact that ϕ is multiplicative, so it immediately shows that if $f : \mathbb{N} \to \mathbb{N}$ is multiplicative then so is $\sum_{d|n} f(d)$.

E.g., $d(n) = \tau(n) = \sum_{d|n} 1$ = number of divisors of n, and $\sigma(n) = \sum_{d|n} d$ = sum of divisors of n are multiplicative.

Let's think about solutions to polynomial congruences. For example:

(i) $x^2 + 2 \equiv 0 \pmod 5 \longrightarrow$ no solutions

(ii) $x^3 + 1 \equiv 0 \pmod 7 \longrightarrow$ three solutions $(3, 5, 6)$

(iii) $x^2 - 1 \equiv 0 \pmod 8 \longrightarrow$ four solutions $(\pm 1, \pm 3)$.

The first example shows that polynomial congruences can have no solutions. The last example illustrates that strange things can happen if we don't work modulo a prime.

But perhaps, modulo a prime, a polynomial congruence does not have too many solutions.

Theorem 14 (Lagrange's Theorem). Let p be a prime and $f(x) = a_n x^n + \ldots + a_1 x + a_0$ be a polynomial with integer coefficients, with a_n not divisible by p.

Then $f(x) \equiv 0 \pmod p$ has at most n solutions.

Remark. We really do need p to be prime.

Proof. (Use/adapt proof from ordinary arithmetic.)

By induction on n: $n = 1$ is a linear congruence – we have already dealt with this.

Assume true for polynomials of degree $n-1$, and let f be a polynomial of degree n as above. If there are no solutions to $f(x) \equiv 0 \pmod p$ then we are done, so assume that there *is* a solution, say x_0.

Recall $x^j - x_0^j = (x - x_0)(x^{j-1} + x^{j-2}x_0 + \ldots + x x_0^{j-2} + x_0^{j-1})$.

So $f(x) \equiv f(x) - f(x_0) \equiv (x - x_0)g(x) \pmod p$, with g a polynomial with integer coefficients and degree $n-1$.

If $f(x_0) \equiv 0 \pmod p$, then $(x - x_0)g(x) \equiv 0 \pmod p$. But $\mathbb{Z}/p\mathbb{Z}$ has no zero divisors (it's a field), so either $x \equiv x_0 \pmod p$ or $g(x) \equiv 0 \pmod p$.

By the induction hypothesis, $g(x) \equiv 0 \pmod p$ has at most $n-1$ solutions, so $f(x) \equiv 0 \pmod p$ has at most n solutions. □

Let's think about $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ where p is prime, and let's think about the orders of the elements of that group. We already know that they divide $p-1$, but can we say more?

For $p = 7$:

element	1	2	3	4	5	6
order	1	3	6	3	6	2

$\Longrightarrow$

order	1	2	3	6
#elements	1	1	2	2

For $p = 13$:

element	1	2	3	4	5	6	7	8	9	10	11	12
order	1	12	3	6	4	12	12	4	3	6	12	2

$\Longrightarrow$

order	1	2	3	4	6	12
#elements	1	1	2	2	2	4

Speculation. Do we always have elements of order $p-1$? Are there always $\phi(d)$ elements of order d?

Theorem 15. Let p be a prime. Then $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ is cyclic.

Proof. Aim: to show that there is an element of order $p-1$.

Idea: show that there are $\phi(d)$ elements of order d, for each d dividing $p-1$.

Let $S_d = \left\{a \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times : a \text{ has order } d\right\}$. (So $S_d = \emptyset$ if $d \nmid p-1$.)

Our aim is: if $d \mid p-1$ then $|S_d| = \phi(d)$.

The sets S_d partition $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$, so $\sum_{d|p-1} |S_d| = p-1$.

Suppose that S_d is non-empty, say $a \in S_d$. So a has order d. Then $1, a, a^2, \ldots, a^{d-1}$ are d distinct elements and they are solutions of $x^d - 1 \equiv 0 \pmod{p}$.

By Lagrange's theorem (Theorem 14) there are at most d solutions to this congruence, so these are all of them. So $S_d \subset \{1, a, a^2, \ldots, a^{d-1}\}$. We want to know which of the elements a^j $(0 \leqslant j \leqslant d-1)$ have order d.

Suppose a^j has order k. Then $k \mid d$. Also $a^{jk} \equiv 1 \pmod{p}$. But a has order d, so $d \mid jk$. If $(j,d) = 1$, then we get $d \mid k$, and $k \mid d$, so $k = d$.

Is it the case that if a^j has order d, then $(j,d) = 1$?

If $(j,d) = m > 1$ then $(a^j)^{d/m} \equiv (a^d)^{j/m} \equiv 1 \pmod{p}$, so a^j has order $d/m < d$.

So $S_d = \{a^j : 0 \leqslant j \leqslant d-1 \text{ and } (j,d) = 1\}$, so $|S_d| = \phi(d)$.

So either $|S_d| = 0$ or $|S_d| = \phi(d)$.

Now $\sum_{d|p-1} \left[\phi(d) - |S_d|\right] = (p-1) - (p-1) = 0$ (using Lemma 12), and $\phi(d) - |S_d| \geqslant 0$, so in fact $|S_d| = \phi(d)$ for all divisors d of $p-1$.

In particular, $|S_{p-1}| = \phi(p-1) \geqslant 1$, so we have an element of order $p-1$. □

Until now our names for the elements of $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ (usually $1, \ldots, p-1$) were good for addition but less so for multiplication. We can now view elements as $1, a, a^2, \ldots, a^{p-2}$, which is better for multiplication.

Definition. If a is a generator for the group $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$, then we say that a is a **primitive root** modulo p.

Lecture 5

We now study $\left(\mathbb{Z}/p^j\mathbb{Z}\right)^\times$.

Try $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$. This has order $\phi(p^2) = p(p-1)$. Is it cyclic?

We know there is a primitive root modulo p, say a. Then $1, a, a^2, \ldots, a^{p-2}$ are all different modulo p, and so are different modulo p^2. But what is the order of a modulo p^2?

Say a has order d modulo p^2. Then, by Lagrange or Fermat-Euler, $d \mid \phi(p^2)$, that is $d \mid p(p-1)$.

Also $a^d \equiv 1 \pmod{p^2}$, so $a^d \equiv 1 \pmod{p}$.

But a has order $p-1$ modulo p, so $p-1 \mid d$ and $d \mid p(p-1)$, so either $d = p-1$ or $d = p(p-1)$.
bad ↗ good ↗

So we want $a^{p-1} \not\equiv 1 \pmod{p^2}$, and then a would be a primitive root modulo p^2.

Lemma 16. Let p be a prime. Then there is a primitive root modulo p, say g, such that $g^{p-1} = 1 + bp$ where $(b, p) = 1$. (So then $g^{p-1} \equiv 1 \pmod{p}$ and $g^{p-1} \not\equiv 1 \pmod{p^2}$.)

Proof. By Theorem 15 we know that *is* a primitive root modulo p, say a. If $a^{p-1} = 1 + bp$ where $(b, p) = 1$ then we are done.

So suppose that $a^{p-1} \equiv 1 \pmod{p^2}$. (This can happen.)

Consider $a + p$, which is still a primitive root modulo p. Then

$$(a+p)^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}p + \text{higher order terms},$$

where the higher order terms are all divisible by p^2. So

$$\begin{aligned}(a+p)^{p-1} &\equiv a^{p-1} + (p-1)a^{p-2}p \pmod{p^2} \\ &\equiv 1 + \underbrace{(p-1)a^{p-2}}_{b}\, p \pmod{p^2} \\ &\not\equiv 1 \pmod{p^2} \quad \text{since } (b,p) = 1\end{aligned}$$

So $a + p$ will do. (I.e., either a or $a + p$ will do). □

because of size, not parity ↙

Lemma 17. Let p be a prime greater than 2 and let j be a natural number. Then there is a primitive root modulo p, say g, such that $g^{p^{j-1}(p-1)} \not\equiv 1 \pmod{p^{j+1}}$.

Proof. By induction on j: $j = 1$ is exactly Lemma 16.

Induction step. Suppose that we have g such that $g^{p^{j-2}(p-1)} \not\equiv 1 \pmod{p^j}$, where $j \geqslant 2$.

(But certainly $g^{p^{j-2}(p-1)} \equiv 1 \pmod{p^{j-1}}$, by Lagrange or Fermat-Euler.)

Then we have

$$g^{p^{j-2}(p-1)} = 1 + b_{j-1}p^{j-1}, \quad \text{where } (b_{j-1}, p) = 1.$$

Then

$$g^{p^{j-1}(p-1)} = \left(1 + b_{j-1}p^{j-1}\right)^p = 1 + b_{j-1}p^j + \text{higher order terms},$$

where the higher order terms are either

- $b_{j-1}^p (p^{j-1})^p$, which is divisible by p^{j+1} for $p \geqslant 3$, or
- $\binom{p}{r} b_{j-1}^r (p^{j-1})^r$ where $2 \leqslant r \leqslant p-1$, which is divisible by p^{j+1}.

So $g^{p^{j-1}(p-1)} \equiv 1 \pmod{p^j}$.

And $g^{p^{j-1}(p-1)} \equiv 1 + b_{j-1}p^j \not\equiv 1 \pmod{p^{j+1}}$, since $(b_{j-1}, p) = 1$. □

Remark. The result is not true when $p = 2$.

In Lemma 16 (case $j = 1$), can take $g = 3$ (then $g \equiv 1 \pmod 2$, $g \not\equiv 1 \pmod 4$). But in case $j = 2$ there is no g such that $g^2 \equiv 1 \pmod 4$ but $g^2 \not\equiv 1 \pmod 8$.

We can now study $\left(\mathbb{Z}/p^j\mathbb{Z}\right)^\times$ for $p \geqslant 3$.

Theorem 18. Let p be a prime greater than 2, and let j be a natural number.

Then $\left(\mathbb{Z}/p^j\mathbb{Z}\right)^\times$ is cyclic.

Proof. Let g be as in Lemma 17. We shall show that g has order $\phi(p^j)$ modulo p^j.

Claim. For $i \geqslant 1$, g has order $p^{i-1}(p-1)$ modulo p^i.

Proof. For $i = 1$, we choose g to be a primitive root modulo p.

Induction step. Suppose that g has order $p^{i-2}(p-1)$ modulo p^{i-1} (where $i \geqslant 2$). Say that g has order d modulo p^i.

Then $d \mid \phi(p^i)$, that is $d \mid p^{i-1}(p-1)$.

Also, $g^d \equiv 1 \pmod{p^i}$, so $g^d \equiv 1 \pmod{p^{i-1}}$.

But g has order $p^{i-2}(p-1)$ modulo p^{i-1}, so $p^{i-2}(p-1) \mid d$.

So $d = p^{i-2}(p-1)$ or $d = p^{i-1}(p-1)$. But $g^{p^{i-2}(p-1)} \not\equiv 1 \pmod{p^i}$ by Lemma 17.

So $d = p^{i-1}(p-1)$. □

Remark. The theorem is not true for $p = 2$. For example, $\left(\mathbb{Z}/8\mathbb{Z}\right)^\times$ is not cyclic ($1, 3, 5, 7$ all have order 1 or 2, so no element has order 4).

Exercises.

1. What is the structure of $\left(\mathbb{Z}/2^j\mathbb{Z}\right)^\times$?
2. For which n is $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ cyclic?
3. If g is a primitive root modulo p^2, must it be a primitive root modulo p?

Example. We saw that 3 is a primitive root modulo 7 (it has order 6).

Also, $3^6 = 729 = 1 + 7 \times 104$ and $(104, 7) = 1$, so $3^6 \not\equiv 1 \pmod{7^2}$, so 3 is a primitive root modulo 7^n for all $n \geqslant 1$.

Lecture 6

We are interested in when the congruence $x^2 \equiv a \pmod{n}$ can be solved. We'll start with the case that $n = p$ is prime.

Definition. Let a be coprime to n. If there is a solution to the congruence $x^2 \equiv a \pmod{n}$ then we say a is a **quadratic residue** modulo n. ("Residue" is too general; need word "quadratic".)

If not, then we say that a is a **quadratic non-residue** modulo n.

Examples. 1 is a quadratic residue for all n.

2 is a quadratic residue modulo 7, since $3^2 \equiv 2 \pmod{7}$, but 2 is a quadratic non-residue modulo 5.

Modulo 7, the quadratic residues are $1, 2, 4$, and the quadratic non-residues are $3, 5, 6$.

Question. How many quadratic residues are there modulo a prime?

Lemma 19. Let p be an odd prime. Then there are exactly $\frac{p-1}{2}$ quadratic residues modulo p (and so $\frac{p-1}{2}$ quadratic non-residues).

Proof 1. There are at most $\frac{p-1}{2}$ quadratic residues since $(-a)^2 \equiv a^2 \pmod{p}$ and $-a \not\equiv a \pmod{p}$ as p is an odd prime. (I.e., can pair them off.)

Are these the only duplicates?

Suppose $x^2 \equiv y^2 \pmod{p}$. We want that $x \equiv \pm y \pmod{p}$.

We have $x^2 - y^2 \equiv 0 \pmod{p} \implies (x + y)(x - y) \equiv 0 \pmod{p}$.

As p is prime, so $x \equiv \pm y \pmod{p}$, so there are exactly $\frac{p-1}{2}$ quadratic residues. □

↑ used; not true in general ↖ useful to know when two numbers have same square

Proof 2. There is a primitive root modulo p, say g. For which i $(0 \leqslant i \leqslant p - 2)$ do we have g^i a quadratic residue? If i is even, say $i = 2j$, then $g^i = (g^j)^2 \pmod{p}$, so g^i is a quadratic residue.

Are these the only values?

Suppose $g^i \equiv x^2 \pmod{p}$ for some x. Then $x = g^k$, say, so $g^i \equiv g^{2k} \pmod{p}$. (This does *not* imply $i = 2k$)

Then $g^{i-2k} \equiv 1 \pmod{p}$, and since g has order $p-1$ modulo p, this gives $p - 1 \mid i - 2k$.

But $p - 1$ is even, so $2 \mid i - 2k$, so $2 \mid i$. (Nice application of quadratic residues.)

So g^i is a quadratic residue iff i is even. □

- QR $\times$ QR $\to$ QR: $\left.\begin{array}{l} a \equiv x^2 \pmod p \\ b \equiv y^2 \pmod p \end{array}\right\} \implies ab \equiv (xy)^2 \pmod p$
- QR $\times$ QNR $\to$ QNR. $\left.\begin{array}{l} a \equiv x^2 \pmod p \\ ab \equiv z^2 \pmod p \end{array}\right\} \implies b \equiv (zx^{-1})^2 \pmod p$
- QNR $\times$ QNR $\to$ QR.

Definition. Let p be a prime and let a be an integer. We define the **Legendre symbol** $\left(\frac{a}{p}\right)$ as follows:

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

We can define $\chi : \begin{array}{ccc} \left(\mathbb{Z}/p\mathbb{Z}\right)^\times & \longrightarrow & \{-1,1\} \\ a & \longmapsto & \left(\frac{a}{p}\right) \end{array}$ $\leftarrow$ group under multiplication

Examples. $\left(\frac{1}{p}\right) = 1$ for all primes p.

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

Theorem 20 (Euler's criterion). Let p be an odd prime, and a an integer. Then

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

Proof. If $a \equiv 0 \pmod p$ then the result is clearly true, so assume $(a,p) = 1$.

By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod p$, so $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod p$.

By Proof 1 of Lemma 19, we know that if $x^2 \equiv 1 \pmod p$ then $x \equiv \pm 1 \pmod p$, so $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$.

Let g be a primitive root modulo p and say $a = g^i$ $(0 \leqslant i \leqslant p-2)$. If $i = 2j$ then $a^{\frac{p-1}{2}} \equiv \left(g^{p-1}\right)^j \equiv 1 \pmod p$.

This gives $\frac{p-1}{2}$ solutions to the congruence $x^{\frac{p-1}{2}} \equiv 1 \pmod p$, so by Lagrange's theorem these are all of the solutions. So

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p & \text{if } a = g^i,\ i \text{ even} \\ -1 \pmod p & \text{if } a = g^i,\ i \text{ odd} \end{cases}$$

But Proof 2 of Lemma 19 showed that g^i is a quadratic residue iff i is even. $\square$

This gives a useful way to get a handle on $\left(\frac{a}{p}\right)$.

Corollary 21. The Legendre symbol is totally multiplicative. That is, if p is prime and a, b are integers, then

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

Consequence: χ is a group homomorphism.

Proof. If $p = 2$, the result is easy to check, so we assume that p is odd.

Then $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \mod p$ by Euler's criterion.

(Note: congruence, not equality.)

But $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ and $\left(\frac{ab}{p}\right)$ are $-1, 0, 1$ and the only way for two of these to be congruent modulo the odd prime p is if they are in fact equal. □

Example. We can use this property to obtain a third proof of Lemma 19.

As in the beginning of Proof 1 of Lemma 19, there is at least one quadratic non-residue modulo p, say b.

$$\begin{aligned}\left(\frac{b}{p}\right)\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) &= \sum_{a=1}^{p-1}\left(\frac{ab}{p}\right) \quad \text{(using total multiplicativity / homomorphism)} \\ &= \sum_{a=1}^{p-1}\left(\frac{a}{p}\right) \quad \text{(as } b, 2b, \ldots, (p-1)b \text{ is } 1, 2, \ldots, (p-1) \text{ in some order)}\end{aligned}$$

But $\left(\frac{b}{p}\right) = -1$, so $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$.

Since $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = \#(\text{quadratic residues}) - \#(\text{quadratic non-residues})$, we are done. □

Corollary 22. Let p be an odd prime. Then $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

That is, $\begin{cases} -1 \text{ is a quadratic residue modulo } p \text{ if } p \equiv 1 \pmod 4 \\ -1 \text{ is a quadratic non-residue modulo } p \text{ if } p \equiv 3 \pmod 4 \end{cases}$

Proof. Apply Euler's criterion with $a = -1$ to get $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$.

But $\left(\frac{-1}{p}\right)$ and $(-1)^{\frac{p-1}{2}}$ are both ± 1, so in this case congruence gives equality. □

Lecture 7 We want to know about $a^{\frac{p-1}{2}}$.

Reminder of a proof of Fermat's Little Theorem.
If a is coprime to p, then $a, 2a, \ldots, (p-1)a$ are the same as $1, 2, \ldots, (p-1)$ modulo p.
Multiply: $a \times 2a \times \cdots \times (p-1)a \equiv 1 \times 2 \times \cdots \times (p-1) \pmod p$
That is: $(p-1)!a^{p-1} \equiv (p-1)! \pmod p$
Since p and $(p-1)!$ are coprime, we have $a^{p-1} \equiv 1 \pmod p$. □

Could we study $a^{\frac{p-1}{2}}$ similarly? Perhaps multiply $a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a$.

Problems.

- We'd need to know what $a, 2a, , \ldots, \left(\frac{p-1}{2}\right)a$ are.
- We'd get $\left(\frac{p-1}{2}\right)!$ and need to cancel.
- We want answer to be $+1$ or -1. Where does the sign come from?

We could shift our attention from $\{0, 1, \ldots, p-1\}$ to $\{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$.

Definition. Fix an odd prime p. Write $\langle b \rangle$ for the unique integer that is congruent to b modulo p and that lies in $[-\frac{1}{2}p, \frac{1}{2}p]$. (Non-standard notation.)

We're interested in $\langle a \rangle, \langle 2a \rangle, \ldots, \langle \left(\frac{p-1}{2}\right) a \rangle$.

Examples.

- $p = 7$, $a = 2$. Then $\langle a \rangle = 2$, $\langle 2a \rangle = -3$, $\langle 3a \rangle = -1$.
- $p = 11$, $a = 4$. Then $\langle a \rangle = 4$, $\langle 2a \rangle = -3$, $\langle 3a \rangle = 1$, $\langle 4a \rangle = 5$, $\langle 5a \rangle = -2$.

Proposition 23 (Gauss' Lemma). Let p be an odd prime, and let a be coprime to p.

Then $\left(\frac{a}{p}\right) = (-1)^\nu$, where $\nu = \#\left\{k : 1 \leqslant k \leqslant \frac{p-1}{2} \text{ and } \langle ka \rangle < 0\right\}$.

That is, compute $\langle a \rangle, \langle 2a \rangle, \ldots, \langle \left(\frac{p-1}{2}\right) a \rangle$ and count how many are negative.

Proof. Consider $\langle a \rangle, \langle 2a \rangle, \ldots, \langle \left(\frac{p-1}{2}\right) a \rangle$.

Can two be the same? No, since no two of $a, 2a, \ldots, \left(\frac{p-1}{2}\right) a$ are congruent modulo p.

Can two differ by a sign? No, because no two of $a, 2a, \ldots, \left(\frac{p-1}{2}\right) a$ sum to 0 modulo p.

So $\langle a \rangle, \langle 2a \rangle, \ldots, \langle \left(\frac{p-1}{2}\right) a \rangle$ are $\pm 1, \pm 2, \ldots, \pm \left(\frac{p-1}{2}\right)$ in some order, where each comes with a definite sign (and ν of them are negative).

So $\left(\frac{p-1}{2}\right)! \, a^{\frac{p-1}{2}} \equiv \langle a \rangle \times \langle 2a \rangle \times \cdots \times \langle \left(\frac{p-1}{2}\right) a \rangle \equiv \left(\frac{p-1}{2}\right)! \, (-1)^\nu \pmod{p}$.

Since p and $\left(\frac{p-1}{2}\right)!$ are coprime, this gives $a^{\frac{p-1}{2}} \equiv (-1)^\nu \pmod{p}$.

By Euler's criterion this gives $\left(\frac{a}{p}\right) \equiv (-1)^\nu \pmod{p}$, and since $\left(\frac{a}{p}\right)$ and $(-1)^\nu$ both come from $\{+1, -1\}$, this gives $\left(\frac{a}{p}\right) = (-1)^\nu$. □

Corollary. Let p be an odd prime. Then $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Proof. By Gauss' Lemma, $\left(\frac{2}{p}\right) = (-1)^\nu$, where $\nu = \#\left\{b : 1 \leqslant b \leqslant \frac{p-1}{2} \text{ and } \langle 2b \rangle < 0\right\}$.

So we must count how many of $\langle 2 \rangle, \langle 4 \rangle, \ldots, \langle p-1 \rangle$ are negative.

But $2, 4, \ldots, p-1 \in \{1, 2, \ldots, p-1\}$, so $\langle 2b \rangle < 0$ if and only if $\frac{p-1}{2} < 2b \leqslant p-1$, which occurs if and only if $\frac{p-1}{4} < b \leqslant \frac{p-1}{2}$. So $\nu = \#\left\{b : \frac{p-1}{4} < b \leqslant \frac{p-1}{2}\right\}$.

We have that either $p = 4k+1$ or $p = 4k+3$, for an integer k.

- If $p = 4k+1$ then $\nu = \#\{b : k < b \leqslant 2k\} = k$
- If $p = 4k+3$ then $\nu = \#\{b : k + \frac{1}{2} < b \leqslant 2k+1\} = k+1$

So it seems to depend on $p \pmod{8}$.

- If $p = 8\ell + 1$ then $\nu = 2\ell$ is even, so $\left(\frac{2}{p}\right) = 1$.
- If $p = 8\ell + 3$ then $\nu = 2\ell + 1$ is odd, so $\left(\frac{2}{p}\right) = -1$.
- If $p = 8\ell + 5$ then $\nu = 2\ell + 1$ is odd, so $\left(\frac{2}{p}\right) = -1$.
- If $p = 8\ell + 7$ then $\nu = 2\ell + 2$ is even, so $\left(\frac{2}{p}\right) = 1$.

So $\left(\frac{2}{p}\right) = \left\{ \begin{array}{rl} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8 \equiv \pm 3 \pmod 8 \end{array} \right\} = (-1)^{\frac{p^2-1}{8}}$. □

Note. This is a good illustration of the way that Gauss' Lemma can be used.

Question. Let p, q be odd primes. Is there a relationship between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$?

Theorem 25 (Law of Quadratic Reciprocity). Let p and q be odd primes.

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

That is: $\left(\frac{q}{p}\right) = \left\{ \begin{array}{ll} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{array} \right.$

Remark. This phrasing includes the case $p = q$ (both sides are then 0).

The result is sometimes phrased as this: if p and q are *distinct* odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Examples.

- $\left(\frac{19}{73}\right) = \left(\frac{73}{19}\right)$ (by quadratic reciprocity, as $73 \equiv 1 \pmod 4$)
  $= \left(\frac{16}{19}\right)$ (as $73 \equiv 16 \pmod{19}$)
  $= 1$ (as $16 \equiv 4^2 \pmod{19}$)
- $\left(\frac{34}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{17}{97}\right)$ (multiplicativity)
  $= (-1)^{\frac{97^2-1}{8}}\left(\frac{97}{17}\right)$ (using $\left(\frac{2}{p}\right)$ and LQR, as $97 \equiv 1 \pmod 4$)
  $= 1 \times \left(\frac{12}{17}\right)$ (as $97 \equiv 1 \pmod 8$ and $97 \equiv 12 \pmod{17}$)
  $= \left(\frac{4}{17}\right)\left(\frac{3}{17}\right)$ (multiplicativity)
  $= 1 \times \left(\frac{17}{3}\right)$ (as $4 \equiv 2^2 \pmod{17}$ and $17 \equiv 1 \pmod 4$)
  $= \left(\frac{2}{3}\right)$ (as $17 \equiv 2 \pmod 3$)
  $= -1$

Lecture 8

Proof of LQR. Idea: use Gauss' Lemma.

$$\left(\frac{q}{p}\right) = (-1)^{\nu} \text{ where } \nu = \#\left\{b : 1 \leqslant b \leqslant \tfrac{1}{2}(p-1) \text{ and } \langle bq \rangle_p < 0\right\}.$$

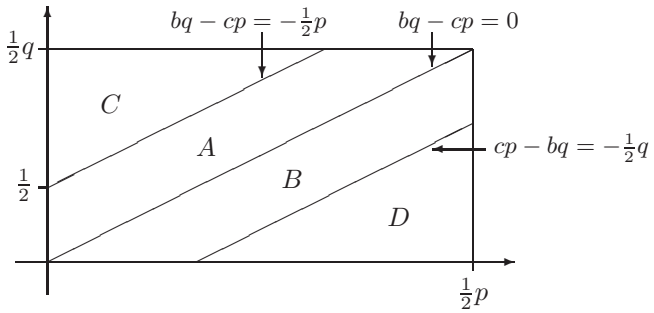
We have $\langle bq \rangle = bq - cp$ for unique integer c. We wish to count (or know parity of) pairs $(b, c) \in \mathbb{Z}^2$ such that $0 < b < \frac{1}{2}p$ and $-\frac{1}{2}p < bq - cp < 0$.

From these inequalities, we have

$$\begin{aligned} -\tfrac{1}{2}p \;<\; bq - cp \quad &\Longrightarrow \quad cp \;<\; bq + \tfrac{1}{2}p \;<\; \tfrac{1}{2}p(q+1) \\ &\Longrightarrow \quad c \;<\; \tfrac{1}{2}(q+1) \\ &\Longrightarrow \quad c \;<\; \tfrac{1}{2}q \;\text{ as } q \text{ odd.} \\ \text{and} \quad bq - cp \;<\; 0 \quad &\Longrightarrow \quad cp \;>\; bq \;>\; 0 \\ &\Longrightarrow \quad c \;>\; 0 \end{aligned}$$

So we are interested in pairs $(b, c) \in \mathbb{Z}^2$ such that

$$0 < b < \tfrac{1}{2}p, \quad 0 < c < \tfrac{1}{2}q, \quad \text{and} \quad -\tfrac{1}{2}p < bq - cp < 0.$$



A = number of lattice points in the box with $-\frac{1}{2}p < bq - cp < 0$.

So we're interested in $\left(\frac{q}{p}\right) = (-1)^A$.

B = number of lattice points in the box with $-\frac{1}{2}q < cp - bq < 0$.

So we're interested in $\left(\frac{p}{q}\right) = (-1)^B$.

Aim: we want $(-1)^A = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(-1)^B$.

That is, we want $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) + B - A$ to be even.

Now, $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ is the number of lattice points in the box.

Let C = number of lattice points in the top-left triangle, and D = number of lattice points in the bottom-right triangle.

We have that $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) + B - A$ is even iff $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) - (A+B) = C + D$ is even.

So if we can show that $C = D$ then we are done. We can define a bijection between points in C and points in D, as follows:

$$b \mapsto \tfrac{1}{2}(p+1) - b, \qquad c \mapsto \tfrac{1}{2}(q+1) - c.$$

A quick check shows this works, and this completes the proof. □

Exercise. Show that if p and q are odd primes with $p \equiv \pm q \pmod{4a}$ then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

(In fact one can deduce this result directly from Gauss' Lemma and use it to prove LQR. See, e.g., Davenport.)

What happens with composite moduli? How should we generalise the Legendre symbol? One key property was multiplicativity, so let's try to keep that.

Definition. Let n be an *odd* number and let a be an integer. We define the **Jacobi symbol** $\left(\frac{a}{n}\right)$ as follows.

Say $n = p_1 \ldots p_k$, where the p_i are (not necessarily distinct) primes. Then

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \times \cdots \times \left(\frac{a}{p_k}\right),$$

where $\left(\frac{a}{p_i}\right)$ is the Legendre symbol.

(If $n = 1$, then the empty product gives $\left(\frac{a}{1}\right) = 1$ for all integers a.)

Examples.

- If $n = p$ is prime, then the Jacobi symbol $\left(\frac{a}{n}\right)$ is just the Legendre symbol $\left(\frac{a}{n}\right)$.
- $\left(\frac{1}{15}\right) = \left(\frac{1}{3}\right)\left(\frac{1}{5}\right) = 1 \times 1 = 1$.
- $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1) \times (-1) = 1$.
- $\left(\frac{3}{15}\right) = \left(\frac{3}{3}\right)\left(\frac{3}{5}\right) = 0$.
- $\left(\frac{4}{15}\right) = \left(\frac{4}{3}\right)\left(\frac{4}{5}\right) = \left(\frac{1}{3}\right) \times 1 = 1 \times 1 = 1$.

Remark ("really important"). It is possible for the Jacobi symbol $\left(\frac{a}{n}\right)$ to be 1 even if a is not a quadratic residue modulo n.

For example, $\left(\frac{2}{15}\right) = 1$, but 2 is not a quadratic residue modulo 15. (If it were, then 2 would be a quadratic residue modulo 3, and it isn't.)

If is true that if $\left(\frac{a}{n}\right) = -1$ then a is a quadratic non-residue modulo n.

It is terribly easy to think that $\left(\frac{a}{n}\right) = 1$ implies a is a quadratic residue modulo n.

Lemma 26. The Jacobi symbol is multiplicative in two senses.

(i) If n is an odd natural number and if a, b are integers, then $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

(ii) If m, n are odd natural numbers and a is an integer, then $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

Proof.

(i) By the definition of the Jacobi symbol and multiplicativity of the Legendre symbol.

(ii) By the definition of the Jacobi symbol.

We studied $\left(\frac{-1}{p}\right)$. What happens with $\left(\frac{-1}{n}\right)$?

Lemma 27. Let n be an odd natural number. Then $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$ and $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Proof.

(i) Say $n = p_1 \ldots p_k$, where the p_i are (not necessarily distinct) primes.
Say that ℓ of the p_i are congruent to -1 modulo 4, so then $k - \ell$ are congruent to $+1$ modulo 4. Then

$$\left(\frac{-1}{n}\right) \;=\; \left(\frac{-1}{p_1}\right) \times \cdots \times \left(\frac{-1}{p_k}\right) \;=\; (-1)^{\ell} \;=\; (-1)^{\frac{n-1}{2}}.$$

$\uparrow$ by result for Legendre symbol

(ii) Say that m of the p_i are congruent to ± 3 modulo 8, so then $k - m$ are congruent to ± 1 modulo 8. Then

$$\left(\frac{2}{n}\right) \;=\; \left(\frac{2}{p_1}\right) \times \cdots \times \left(\frac{2}{p_k}\right) \;=\; (-1)^{m} \;=\; (-1)^{\frac{n^2-1}{8}}.$$

$\uparrow$ by result for Legendre symbol $\square$

Slogan. "To prove a result for the Jacobi symbol, use the definition of the Jacobi symbol and the corresponding result for the Legendre symbol."

What happens with quadratic reciprocity?

Theorem 28 (LQR for Jacobi symbol). Let m and n be odd natural numbers.

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

Remark. To phrase it as $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$, we must insist that m, n are coprime.

Lecture 9

Proof. (Use our slogan.) Let $n = p_1 \ldots p_k$ and $m = q_1 \ldots q_\ell$, where the p_i, q_j are (not necessarily distinct) primes. Then

$$\begin{aligned}
\left(\frac{m}{n}\right) &= \prod_{i=1}^{k} \left(\frac{m}{p_i}\right) \quad \text{(definition)} \\
&= \prod_{i=1}^{k} \prod_{j=1}^{\ell} \left(\frac{q_j}{p_i}\right) \quad \text{(multiplicativity)} \\
&= \prod_{i=1}^{k} \prod_{j=1}^{\ell} (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} \left(\frac{p_i}{q_j}\right) \quad \text{(LQR for Legendre symbol)} \\
&= (-1)^{\alpha} \prod_{i=1}^{k} \prod_{j=1}^{\ell} \left(\frac{p_i}{q_j}\right) \\
&= (-1)^{\alpha} \left(\frac{n}{m}\right)
\end{aligned}$$

where $(-1)^{\alpha} = \prod_{i=1}^{k} \prod_{j=1}^{\ell} (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}$.

Say r of the p_i are congruent to $-1 \pmod 4$, so that $k - r$ are congruent to $1 \pmod 4$. And s of the q_j are congruent to $-1 \pmod 4$, so that $\ell - s$ are congruent to $1 \pmod 4$.

Then we count -1 in $(-1)^\alpha$ exactly when p_i and q_j are both $-1 \pmod 4$, and 1 otherwise.

So $(-1)^\alpha = (-1)^{rs} = \begin{cases} 1 & \text{if } r \text{ is even or } s \text{ is even} \\ -1 & \text{if } r, s \text{ are both odd} \end{cases}$.

But $n \equiv 1 \pmod 4$ iff r is even, and $m \equiv 1 \pmod 4$ iff s is even.

So $(-1)^\alpha = \left\{ \begin{array}{ll} 1 & \text{if } m \equiv 1 \pmod 4 \text{ or } n \equiv 1 \pmod 4 \\ -1 & \text{if } m, n \equiv -1 \pmod 4 \end{array} \right\} = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$. □

Example.
$$\begin{aligned} \left(\tfrac{33}{73}\right) &= \left(\tfrac{73}{33}\right) && \text{(by LQR, as } 73 \equiv 1 \pmod 4) \\ &= \left(\tfrac{7}{33}\right) && \text{(as } 73 \equiv 7 \pmod{33}) \\ &= \left(\tfrac{33}{7}\right) && \text{(by LQR, as } 33 \equiv 1 \pmod 4) \\ &= \left(\tfrac{5}{7}\right) && \text{(as } 33 \equiv 5 \pmod 7) \\ &= \left(\tfrac{7}{5}\right) && \text{(by LQR, as } 5 \equiv 1 \pmod 4) \\ &= \left(\tfrac{2}{5}\right) && \text{(as } 7 \equiv 2 \pmod 5) \\ &= -1 \end{aligned}$$

Key point: we did not use the fact that anything was prime; no need to worry about factorising.

Binary Quadratic Forms

Question. Which numbers can be expressed as the sum of two squares? That is, which numbers can be written as $n = x^2 + y^2$ for some integers x, y?

Definition. A **binary quadratic form** is an expression $f(x, y) = ax^2 + bxy + cy^2$, where the coefficients a, b, c are integers, and we are interested in integer variables x, y.

We may write this f as (a, b, c), and we can write f in terms of a matrix:

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

Examples.

- $f(x, y) = x^2 + y^2$, written as $(1, 0, 1)$ or $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- $f(x, y) = 4x^2 + 12xy + 9y^2$, written as $(4, 12, 9)$ or $\begin{pmatrix} 4 & 6 \\ 6 & 9 \end{pmatrix}$.

Let's try $f(x, y) = 4x^2 + 12xy + 10y^2 = (2x + 3y)^2 + y^2$.

Do $4x^2 + 12xy + 10y^2$ and $X^2 + Y^2$ represent the same numbers?

Put $X = 2x + 3y$, $Y = y$. Then $\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$, so $\begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & -3 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$.

Ah. There are integer values of X, Y that don't give integer values of x, y.

But $4x^2 + 12xy + 10y^2 = 2(x+y)^2 + 2(x+2y)^2$.

Try $\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$, so $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$.

So $(4, 12, 10)$ and $(2, 0, 2)$ represent the same numbers.

Definition. A **unimodular substitution** is one of the form $X = px + qy$, $Y = rx + sy$, where p, q, r, s are integers with $ps - qr = 1$.

Equivalently, $\begin{pmatrix} X \\ Y \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$, where $A \in SL_2(\mathbb{Z})$.

Reminder: the special linear group, $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} p & q \\ r & s \end{pmatrix} : p, q, r, s \in \mathbb{Z},\ ps - qr = 1 \right\}$.

Remark. We don't allow substitutions corresponding to matrices with det $= -1$.

Exercise. Check that there are integers r, s such that $\begin{pmatrix} 2 & 3 \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$.

Definition. We say that two binary quadratic forms $f(x, y) = ax^2 + bxy + cy^2$ and $f'(x, y) = a'x^2 + b'xy + c'y^2$ are **equivalent** if they are related by a unimodular substitution.

In this case, we write $f \sim f'$, or $(a, b, c) \sim (a', b', c')$.

In matrix terms, if $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$, then

$$\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} p & q \\ r & s \end{pmatrix}^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

are equivalent.

Examples. $(4, 12, 9) \sim (1, 0, 0)$ and $(4, 12, 10) \sim (2, 0, 2)$.

(The point is that equivalent forms represent the same numbers.)

Exercise. Check that equivalence of binary quadratic forms is an equivalence relation.

Definition. The **discriminant** of the binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is $\text{disc}(f) = b^2 - 4ac$.

Examples.

- $\text{disc}(1, 0, 1) = -4$
- $\text{disc}(4, 12, 9) = \text{disc}(1, 0, 0) = 0$.
- $\text{disc}(4, 12, 10) = \text{disc}(2, 0, 2) = -16$.

Lemma 29. Equivalent binary quadratic forms have the same discriminant.

Proof. Say $f(x, y) = ax^2 + bxy + cy^2$. Let $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$.

$$\begin{aligned}\text{Then}\quad f'(x,y) &= a(px+qy)^2 + b(px+qy)(rx+sy) + c(rx+sy)^2 \quad . \\ &= (ap^2+bpr+cr^2)x^2 + (2apq+brq+bps+2crs)xy \\ &\quad +(aq^2+bqs+cs^2)y^2\end{aligned}$$

$$\begin{aligned}\text{So}\quad \text{disc}(f') &= (2apq+brq+bps+2crs)^2 - 4(ap^2+bpr+cr^2)(aq^2+bqs+cs^2) \ . \\ &= (b^2-4ac)(ps-qr)^2\end{aligned}$$

But $ps-qr=1$, so $\text{disc}(f') = b^2-4ac = \text{disc}(f)$. □

An alternative proof... If $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$. We have $\text{disc}(f) = -4\det\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$.

So if f' corresponds to $\begin{pmatrix} p & q \\ r & s \end{pmatrix}^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix}$, then

$$\begin{aligned}\text{disc}(f') &= -4\det\left(\begin{pmatrix} p & q \\ r & s \end{pmatrix}^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix}\right) \\ &= -4\det\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = \text{disc}(f)\end{aligned}$$

□

Lecture 10

Remark. The converse is not true. There are binary quadratic forms with the same discriminant that are not equivalent. For example, the forms $(1,0,6)$ and $(2,0,3)$ both have discriminant -24. We can see that $(1,0,6)$ represents 1 (via $x=1, y=0$), but $(2,0,3)$ certainly does not. So they are not equivalent. (Discriminants are useful, but don't tell us everything.)

What numbers can be the discriminant of a binary quadratic form?

Lemma 30. There is a binary quadratic form with discriminant d if and only if d is congruent to 0 or 1 modulo 4.

Proof. ($\Rightarrow$). If $d = b^2-4ac$ then $d \equiv b^2 \pmod 4$, so $d \equiv 0$ or $1 \pmod 4$.

($\Leftarrow$). If $d \equiv 0 \pmod 4$ then it is the discriminant of $(1,0,-\frac{d}{4})$.

If $d \equiv 1 \pmod 4$ then it is the discriminant of $(1,0,\frac{1-d}{4})$. □

If $f(x) = ax^2+bx+c$ has discriminant $d = b^2-4ac$ then

$$4af(x) = 4a^2x^2+4abx+4ac = (2ax+b)^2 + (4ac-b^2)$$

- If $d > 0$ then $f(x)$ can be either positive or negative.
- If $d < 0$ then $4af(x) \geqslant 0$ for all x.

Definition. Let f be a binary quadratic form with non-zero discriminant. We say that f is

- **positive definite** if $f(x,y) \geqslant 0$ for all x, y
- **negative definite** if $f(x,y) \leqslant 0$ for all x, y
- **indefinite** if $f(x,y) > 0$ for some x, y and $f(x',y') < 0$ for some x', y'.

(Zero-discriminant is not interesting.)

Lemma 31. Let $f(x,y) = ax^2 + bxy + cy^2$ be a binary quadratic form with discriminant $d = b^2 - 4ac$ and with $a \neq 0$.

- If $d < 0$ and $a > 0$ then f is positive definite.
- If $d < 0$ and $a < 0$ then f is negative definite.
- If $d > 0$ then f is indefinite.

Proof. Idea: do similar as for quadratics in one variable.

$$4af(x,y) = 4a^2x^2 + 4abxy + 4acy^2 = (2ax+by)^2 + \underbrace{(4ac - b^2)}_{-d}y^2.$$

(i) If $d < 0$ then $4af(x,y) \geqslant 0$ for all x, y, with equality iff $x = y = 0$. So

- if $d < 0$, $a > 0$ then $f(x,y) \geqslant 0$ for all x, y, with equality iff $x = y = 0$
- if $d < 0$, $a < 0$ then $f(x,y) \leqslant 0$ for all x, y, with equality iff $x = y = 0$.

(ii) If $d > 0$ then

$$\begin{aligned} 4af(x,y) &= (2ax+by)^2 - dy^2 \\ &= \big(2ax + by - y\sqrt{d}\big)\big(2ax + by + y\sqrt{d}\big) \\ &= 4a^2\left(x + y(b-\sqrt{d})/2a\right)\left(x + y(b+\sqrt{d})/2a\right) \\ &= 4a^2(x - \theta y)(x - \phi y) \end{aligned}$$

where $\theta = -(b-\sqrt{d})/2a$, $\phi = -(b+\sqrt{d})/2a$.

If $\big(\frac{x}{y} < \theta$ and $\frac{x}{y} < \phi\big)$ or $\big(\frac{x}{y} > \theta$ and $\frac{x}{y} > \phi\big)$, then the brackets have the same sign and so $4af(x,y) > 0$.

If $\theta < \frac{x}{y} < \phi$ or $\phi < \frac{x}{y} < \theta$, then the brackets have different signs are so $4af(x,y) < 0$. □

Remark. It is possible to have a form whose coefficients are all positive but nevertheless is indefinite. E.g., $(1,3,1)$, which has discriminant $3^2 - 4 \times 1 \times 1 > 0$.

It is also possible to have a form where not all of the coefficients are positive but that is positive definite. E.g., $(1,-1,2)$.

If (a,b,c) is a positive definite form then $a > 0$ and $b^2 - 4ac < 0$, so $c > 0$. From now on, we shall concentrate on positive definite binary quadratic forms.

We have an equivalence relation $\sim$ on positive definite binary quadratic forms, so each form belongs to an equivalence class. Our aim now is to find a "simple" representation of each equivalence class.

Let's think about $(10, 34, 29)$. The middle coefficient is very large – can we decrease it?

Try the substitution $T_\pm$ corresponding to the matrix $\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$. This sends $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ to

$$\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix} \begin{pmatrix} a & b/2 \pm a \\ b/2 & c \pm b/2 \end{pmatrix} = \begin{pmatrix} a & b/2 \pm a \\ b/2 \pm a & a \pm b + c \end{pmatrix}$$

So $(a,b,c) \overset{T_\pm}{\sim} (a, b \pm 2a, a \pm b + c)$.

So $(10,34,29) \overset{T_-}{\sim} (10,14,5) \overset{T_-}{\sim} (10,-6,1)$.

Try substitution S, corresponding to $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. This sends $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ to

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} b/2 & -a \\ c & -b/2 \end{pmatrix} = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix}$$

So $(a,b,c) \overset{S}{\sim} (c,-b,a)$.

So $(10,-6,1) \overset{S}{\sim} (1,6,10) \overset{T_-}{\sim} (1,4,5) \overset{T_-}{\sim} (1,2,2) \overset{T_-}{\sim} (1,0,1)$.

We could apply $S, T_\pm$ in different orders. Try this at home!

- Can ensure $a \leqslant c$ (via S).
- Can ensure $|b| \leqslant a$ (via $T_\pm$).

Definition. We say that the positive definite binary quadratic form (a,b,c) is **reduced** if either $-a < b \leqslant a < c$ or $0 \leqslant b \leqslant a = c$.

Lemma 32. Every positive definite binary quadratic form is equivalent to a reduced form.

Lecture 11

Proof. We have unimodular substitutions, $\begin{array}{l} S : (a,b,c) \mapsto (c,-b,a) \\ T_\pm : (a,b,c) \mapsto (a, b \pm 2a, a \pm b + c) \end{array}$.

- If $a > c$, use S to decrease a while keeping $|b|$ fixed.
- If $a < c$ and $|b| > a$, then use T_+ or T_- to decrease $|b|$ while keeping a fixed.

Repeat these steps as long as necessary. Each step decreases $a + |b|$ (while keeping it positive), so this algorithm must stop.

So we see that our original form is equivalent to (a,b,c) with $|b| \leqslant a \leqslant c$.

If $b = -a$, then we can apply T_+ to make the middle coefficient $+a$ while leaving the others unchanged.

If $a = c$, then apply S if necessary to ensure the middle coefficient is non-negative. □

Can two reduced forms be equivalent?

We saw an example of $(1,0,6)$ and $(2,0,3)$. These are both reduced forms of discriminant -24 but not equivalent.

More generally, if $f(x,y) = ax^2 + bxy + cy^2$ is reduced, what can we say about the small numbers it represents? We have

$$f(0,0) = 0, \quad f(1,0) = a, \quad f(0,1) = c.$$

What if neither variable is 0?

Lemma 33. Let $f(x,y) = ax^2 + bxy + cy^2$ be a reduced positive definite binary quadratic form. Then the smallest integers represented by f for coprime x, y, or $x = y = 0$, are 0, a, c, and $a - |b| + c$, in that order.

Proof. We have

$$f(0,0) = 0, \quad f(1,0) = a, \quad f(0,1) = c,$$

and since f is reduced, we have $0 < a \leqslant c$.

If $x = 0$, the coprimality condition forces $y = \pm 1$. Likewise if $y = 0$.

If $|x| \geqslant |y| > 0$, then

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

Similarly, if $|y| \geqslant |x|$, then $f(x,y) \geqslant a - |b| + c$. We can achieve equality, e.g. $f(1, \pm 1)$ gives $a - |b| + c$ (choose sign depending on sign of b).

Since f is reduced, we have $a - |b| + c \geqslant 0$. □

We can then use this to compare reduced forms.

Theorem 34. Every positive definite binary quadratic form is equivalent to a unique reduced form.

Proof. By Lemma 32, every such form is equivalent to some reduced form. It suffices to check that no two reduced forms are equivalent.

Suppose that $f(x,y) = ax^2 + bxy + cy^2$ and $f'(x,y) = a'x^2 + b'xy + c'y^2$ are equivalent reduced forms. We aim to show $a = a'$, $b = b'$, $c = c'$.

By Lemma 33, the smallest non-zero integer represented by f is a, and that by f' is a'. So $a = a'$.

We have $f(\pm 1, 0) = a$, $f(0, \pm 1) = c$ and $f'(\pm 1, 0) = a'$, $f'(0, \pm 1) = c'$ as the smallest non-zero values represented by coprime x, y.

So the four pairs $(\pm 1, 0)$ and $(0, \pm 1)$ for f must correspond to four pairs for f', so we have $c' = c$.

Since $f \sim f'$, they have the same discriminant. So $b^2 - 4ac = b'^2 - 4a'c' = b'^2 - 4ac$, so $b'^2 = b^2$ and hence $b' = \pm b$.

If $b = 0$ then we're done. If $b > 0$ can (a, b, c) and $(a, -b, c)$ both be reduced?

If they are both reduced, then

- $a < c$ (if $a = c$ then middle coefficients must be non-negative).
- $|b| < a$ (cannot have $b = -a$)

So $0 < a < c < a - |b| + c$.

So $f(x,y) = a$ iff $(x,y) = (\pm 1, 0)$
$f(x,y) = c$ iff $(x,y) = (0, \pm 1)$

So $(\pm 1, 0)$ for one form must correspond to $(\pm 1, 0)$ for the other, and likewise for $(0, \pm 1)$.

If the two forms are equivalent via the substitution $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$, where $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$, then we have

$$\begin{pmatrix} \pm 1 \\ 0 \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} \pm 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \pm p \\ \pm r \end{pmatrix}, \quad \text{so } p = \pm 1 \text{ and } r = 0,$$

$$\text{and} \quad \begin{pmatrix} 0 \\ \pm 1 \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 0 \\ \pm 1 \end{pmatrix} = \begin{pmatrix} \pm q \\ \pm s \end{pmatrix}, \quad \text{so } q = 0 \text{ and } s = \pm 1.$$

But $ps - qr = 1$, so $\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so $b = -b$, so $b = 0$. □

So we have a unique representation of each equivalence class of positive definite binary quadratic forms.

Question. How many reduced forms are there with given discriminant?

Example. $d = -24$. Want (a,b,c) such that $b^2 - 4ac = -24$ and $|b| \leqslant a \leqslant c$. (Not exactly the condition for reduced forms, but a good start.)

If (a,b,c) satisfies these conditions, then

$$-24 = b^2 - 4ac \leqslant ac - 4ac \leqslant -3a^2$$

So $a^2 \leqslant 8$, so $a \leqslant 2$. Also, $b^2 - 4ac = b^2 = 0 \pmod 4$, so b is even.

- $a = 1$. Want $b^2 - 4c = -24$.
  Since b is even and $|b| \leqslant a$, the only possibility is $b = 0$, which gives $c = 6$, and $(1,0,6)$ works.
- $a = 2$. Want $b^2 - 8c = -24$.
  If $b = 0$, then $c = 3$, and $(2,0,3)$ works.
  If $b = 2$, then $4 - 8c = -24$, so no integer solutions.

So the only reduced forms with discriminant -24 are $(1,0,6)$ and $(2,0,3)$.

Proposition 35. Let d be a fixed negative integer. Then there are finitely many reduced forms with discriminant d.

Proof. We want (a,b,c) such that $b^2 - 4ac = d$ and $|b| \leqslant a \leqslant c$. (Reduced form is quicker.)

Then $d = b^2 - 4ac \leqslant ac - 4ac \leqslant -3a^2$, so $a^2 \leqslant -d/3$.

So there are finitely many possibilities for a. But $|b| \leqslant a$, there are finitely many possibilities for b. And $c = (b^2 - d)/4a$, so is determined by a, b and d. □

Definition. Let d be a negative integer. The **class number of** d, denoted by $h(d)$, is the number of reduced forms of discriminant d. Equivalently, it is the number of equivalence classes of positive definite binary quadratic forms of discriminant d.

Example. $h(-24) = 2$.

Remarks.

1. Proposition 35 gives existence for $h(d)$ and a way to compute it, although it may take a while.
2. The class number will appear in the *Number Fields* course too.

**** Non-examinable section ****

We might ask what are the discriminants d with a certain class number $h(d)$.

What happens to $h(d)$ as $d \to -\infty$? A conjecture of Gauss: $h(d) \to \infty$ as $d \to -\infty$. (This is known as Gauss' **class number problem**.)

This has led to a lot of interesting number theory.

- E.g., what are the discriminants with class number 1? (There are just 9.)
- Generalised Riemann Hypothesis (GRH) $\implies$ $h(d) \to \infty$ as $d \to -\infty$ (1905).
  And in 1930, GRH false $\implies$ $h(d) \to \infty$ as $d \to -\infty$.

End of non-examinable section

Lecture 12

Lemma 36. Let $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$, where $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$.

Then x', y' are coprime iff x, y are coprime.

Proof. ($\Rightarrow$). If x, y have highest common factor d, then $x' = px + qy$ and $y' = rx + sy$ are both divisible by d. So if $(x', y') = 1$ then $(x, y) = 1$.

($\Leftarrow$). We have $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}^{-1} \begin{pmatrix} x' \\ y' \end{pmatrix}$, with $\begin{pmatrix} p & q \\ r & s \end{pmatrix}^{-1} \in SL_2(\mathbb{Z})$. So it follows immediately from above. □

If x, y are both divisible by $d > 1$ then $f(x, y)$ will be divisible by d^2, so we will concentrate on coprime x and y.

Definition. Let f be a binary quadratic form and n be an integer. We say that f **represents** n if $f(x, y) = n$ for some integers x, y. We say that f **properly represents** n if $f(x, y) = n$ for some *coprime* integers x, y.

Remark. We know that equivalent forms represent the same numbers. Lemma 36 shows that equivalent forms *properly* represent the same numbers.

- Fix n. Which forms properly represent n?
- Fix f. Which numbers are properly represented by f?

Which forms properly represent 1?

If the first coefficient of f is 1 then $f(1,0) = 1$, so f properly represents 1. So any form equivalent to a form with first coefficient 1 must also properly represent 1.

Is that all? That is, if f is a binary quadratic form that properly represents 1, must it be equivalent to a form with first coefficient 1?

Say $f(x,y) = 1$, where x, y are coprime. Does (x,y) correspond to $(1,0)$ under a unimodular substitution? If so, then f is equivalent to a form f' with $f'(1,0) = f(x,y) = 1$.

So, is there a matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$ such that $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} p \\ r \end{pmatrix}$?

Put $p = x$, $r = y$. Can we solve $xs - qy = 1$? Yes, by Bézout, since x, y coprime.

Lemma 37. Let n be a natural number. Then n is properly represented by a form f iff f is equivalent to a form with first coefficient n.

Proof. ($\Leftarrow$). If f is equivalent to f', where f' has first coefficient n, then $f'(1,0) = n$, so f' properly represents n, so f properly represents n.

($\Rightarrow$). If $f(x,y) = n$, where x, y are coprime, then there are integers q, s such that $xs - qy = 1$, by Bézout.

So then $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x & q \\ y & s \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, where $\begin{pmatrix} x & q \\ y & s \end{pmatrix} \in SL_2(\mathbb{Z})$.

So f is equivalent to a form f' with $f'(1,0) = f(x,y) = n$, and therefore f' has first coefficient n. □

Which numbers are represented by $x^2 + xy + y^2$?

From Lemma 37, we see that n is represented iff there is a form with first coefficient n that is equivalent to $(1,1,1)$. When are there b, c such that $(n,b,c) \sim (1,1,1)$?

If $(n,b,c) \sim (1,1,1)$ then (n,b,c) has discriminant $b^2 - 4nc = -3$, so $b^2 \equiv -3 \pmod{4n}$.

What happens if we know that there is a solution to this congruence? Then there are integers b, c such that $b^2 - 4nc = -3$, so that (n,b,c) is a form with discriminant -3.

But we do not know that $(n,b,c) \sim (1,1,1)$. All we know is that (n,b,c) is equivalent to a reduced form of discriminant -3. What are they?

We want (A,B,C) such that $B^2 - 4AC = -3$ and $|B| \leqslant A \leqslant C$. Then $-3 = B^2 - 4AC \leqslant -3A^2$, so $A^2 \leqslant 1$, so $A = 1$.

Then B satisfies $|B| \leqslant 1$ and $B^2 \equiv -3 \pmod 4$. So B odd, but $B \neq -A$, so $B = 1$.

Then $C = (B^2 + 3)/4A = 1$. So the only reduced form of discriminant -3 is $(1,1,1)$, i.e. $h(-3) = 1$.

So every positive definite form of discriminant -3 is equivalent to $(1,1,1)$.

So there is a form $(n,b,c) \sim (1,1,1)$ iff there is a solution to $w^2 \equiv -3 \pmod{4n}$.

Theorem 38. Let n be a natural number.

(any form)

(i) Suppose that n is properly represented by a form of discriminant d. Then there is a solution to the congruence $w^2 \equiv d \pmod{4n}$.

(ii) Suppose that there is a solution to the congruence $w^2 \equiv d \pmod{4n}$. Then there is a form of discriminant d that properly represents n.

(some form, we can't choose it)

Proof.

(i) Say n is properly represented by f of discriminant d. Then f is equivalent to a form f' with first coefficient n, by Lemma 37. Say $f'(x, y) = nx^2 + b'xy + c'y^2$.

Then f' has the same discriminant as f, so $b'^2 - 4nc' = d$, so $b^2 \equiv d \pmod{4n}$.

(ii) Suppose that there is a solution to the congruence $w^2 \equiv d \pmod{4n}$. Then there are integers b, c such that $b^2 = d + 4nc$. Then (n, b, c) is a form of discriminant d, and it properly represents n. □

Example. Which natural numbers can be properly represented as the sum of two squares?

Put $f(x, y) = x^2 + y^2$, i.e. the form $(1, 0, 1)$.

By Theorem 38, if n is properly represented by $(1, 0, 1)$ then there is a solution to $w^2 \equiv -4 \pmod{4n}$, and if there is a solution to this congruence then n is properly represented by some form of discriminant -4.

What are the reduced forms of discriminant -4? We want (a, b, c) such that $b^2 - 4ac = -4$ and $|b| \leqslant a \leqslant c$.

So $-4 \leqslant -3a^2$, so $a^2 \leqslant 4/3$, so $a = 1$. And b must be even, so $b = 0$.

And $c = (b^2 + 4)/4a = 1$, so $(1, 0, 1)$ is the only reduced form of discriminant -4.

So Theorem 38 tells us that n is properly represented by $(1, 0, 1)$ iff there is a solution to $w^2 \equiv -4 \pmod{4n}$. This happens iff there is a solution to $v^2 \equiv -1 \pmod{n}$.

Caution. Take care with $\left(\frac{-1}{n}\right)$ as it's a Jacobi symbol. This congruence having a solution is *not* the same as $\left(\frac{-1}{n}\right) = 1$.

Lecture 13

We see from Theorem 38 that if we want to know which numbers are properly represented by which forms, then it would be a good idea to study the congruence $w^2 \equiv d \pmod{4n}$. More precisely, for fixed d and n we want to know whether this congruence has a solution.

Examples.

1. The natural number n is properly represented by the form $x^2 + xy + y^2$ iff there is a solution to $w^2 \equiv -3 \pmod{4n}$.

2. The natural number n is properly represented by the form $x^2 + y^2$ iff there is a solution to $v^2 \equiv -1 \pmod{n}$.

The key point in each case is that the class number is 1, i.e. there is only one reduced form with the right discriminant.

1. What can we say about $w^2 \equiv -3 \pmod{4n}$?

   Let's study the case when $n = p$ is an odd prime. By the Chinese Remainder theorem there is a solution to $w^2 \equiv -3 \pmod{4p}$ iff there is a solution to

   $$\begin{aligned} w^2 &\equiv -3 \pmod 4 \\ w^2 &\equiv -3 \pmod p \end{aligned}$$

   There is clearly a solution to $w^2 \equiv -3 \pmod 4$, namely $w = 1$. So we can concentrate on $w^2 \equiv -3 \pmod p$. This has a solution iff $\left(\frac{-3}{p}\right) = 1$ or $p = 3$.

   Now

   $$\begin{aligned} \left(\frac{-3}{p}\right) = 1 &\iff \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1 \\ &\iff (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = 1 \quad \text{(by Corollary 22 and LQR)} \\ &\iff \left(\frac{p}{3}\right) = 1 \\ &\iff p \equiv 1 \pmod 3 \end{aligned}$$

   So an odd prime p is properly represented by $(1,1,1)$ iff $p = 3$ or $p \equiv 1 \pmod 3$.

2. This time we study $v^2 \equiv -1 \pmod n$. Focus on the case when $n = p$ is prime.

   Then $v^2 \equiv -1 \pmod p$ has a solution iff $\left(\frac{-1}{p}\right) = 1$, and this happens iff $p = 2$ or $p \equiv 1 \pmod 4$.

   So the prime p is properly represented by $(1,0,1)$ iff $p = 2$ or $p \equiv 1 \pmod 4$.

What happens with $v^2 \equiv -1 \pmod{p^j}$? If this has a solution then there is a solution to $v^2 \equiv -1 \pmod p$. What about the converse?

There is a fairly general result that will be helpful here...

Proposition 39 (Hensel's Lemma). Let f be a polynomial with integer coefficients, and let p be an odd prime. Suppose there is x_1 such that $f(x_1) \equiv 0 \pmod p$ and $f'(x_1) \not\equiv 0 \pmod p$.

Then for each $r \geqslant 1$, there is x_r such that $f(x_r) \equiv 0 \pmod{p^r}$.

Slogan. "If we have a suitable solution modulo p, then we can bootstrap it to a solution modulo p^r." (Surprising!)

Proof. We shall show, by induction on r, that there is x_r such that $f(x_r) \equiv 0 \pmod{p^r}$ and $x_r \equiv x_1 \pmod p$ (so that $f'(x_r) \not\equiv 0 \pmod p$).

Case $r = 1$: this was precisely the supposition in the statement.

Inductive step. Suppose we have x_{r-1} such that $f(x_{r-1}) \equiv 0 \pmod{p^{r-1}}$ and $x_{r-1} \equiv x_1 \pmod p$, so that $f'(x_{r-1}) \not\equiv 0 \pmod p$. (Here, $r \geqslant 2$.)

Then $f(x_{r-1}) = kp^{r-1}$ for some integer k.

Consider $x_r = x_{r-1} + \lambda p^{r-1}$, where λ is an integer.

(If $f(x_r) \equiv 0 \pmod p$ then $f(x_r) \equiv 0 \pmod{p^{r-1}}$.)

Then clearly $x_r \equiv x_{r-1} \equiv x_1 \pmod{p}$. We have

(Taylor series, higher order terms are divisible by $p^{2(r-1)}$ and so by p^r.)

$$\begin{aligned} f(x_r) &= f(x_{r-1} + \lambda p^{r-1}) \\ &\equiv f(x_{r-1}) + \lambda p^{r-1} f'(x_{r-1}) \pmod{p^r} \\ &\equiv p^{r-1}\big(k + \lambda f'(x_{r-1})\big) \pmod{p^r} \end{aligned}$$

So $f(x_r) \equiv 0 \pmod{p^r}$ iff $k + \lambda f'(x_{r-1}) \equiv 0 \pmod{p}$.

Since $f'(x_{r-1}) \not\equiv 0 \pmod{p}$, it has a multiplicative inverse, so we can solve for λ. □

We are interested in the case $f(x) = x^2 + 1$, so $f'(x) = 2x$. Hensel's Lemma cannot help here when $p = 2$, but should help for odd primes.

Let p be an odd prime. Then $v^2 \equiv -1 \pmod{p}$ has a solution iff $p \equiv 1 \pmod{4}$. Using Hensel's Lemma, if $p \equiv 1 \pmod{4}$, then there is v_1 such that $v_1^2 \equiv -1 \pmod{p}$ and $2v_1 \not\equiv 0 \pmod{p}$.

So for $j \geqslant 1$ there is a solution to $v^2 \equiv -1 \pmod{p^j}$.

What happens when $p = 2$? Clearly there *is* a solution to $v^2 \equiv -1 \pmod{2}$.

If $j \geqslant 2$, then a solution to $v^2 \equiv -1 \pmod{2^j}$ would give a solution to $v^2 \equiv -1 \pmod{4}$, which does not exist.

So we have proved:

Theorem 40. The natural number n can be written as the sum of two coprime squares iff n is not divisible by 4 and all odd prime factors of n are congruent to 1 modulo 4.

Summary of proof.

1. n is properly represented by $(1, 0, 1)$ iff there is a solution to $w^2 \equiv -4 \pmod{4n}$ (by Theorem 38, since $(1, 0, 1)$ is the only reduced form of discriminant -4).

2. This happens iff there is a solution to $v^2 \equiv -1 \pmod{n}$.

3. Let $n = 2^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, where p_i are distinct odd primes, $\alpha_1 \geqslant 0$, and $\alpha_i \geqslant 1$ for $2 \leqslant i \leqslant k$.

   Then there is a solution to $v^2 \equiv -1 \pmod{n}$ iff there is a solution to

$$\left.\begin{array}{ll} v^2 \equiv -1 & \pmod{2^{\alpha_1}} \\ v^2 \equiv -1 & \pmod{p_2^{\alpha_2}} \\ \quad\vdots & \\ v^2 \equiv -1 & \pmod{p_k^{\alpha_k}} \end{array}\right\} \text{Chinese Remainder Theorem}$$

4. There is a solution to $v^2 \equiv -1 \pmod{p_i}$ iff $p_i \equiv 1 \pmod{4}$.

5. There is a solution to $v^2 \equiv -1 \pmod{p_i^{\alpha_i}}$ iff there is a solution to $v^2 \equiv -1 \pmod{p_i}$.

6. There is a solution to $v^2 \equiv -1 \pmod{2^{\alpha_1}}$ iff $\alpha_1 \in \{0, 1\}$. □

Corollary 41. The natural number n is a sum of two squares iff each prime congruent to 3 modulo 4 occurring in the prime factorisation of n occurs to an even power.

Proof. We know that n is the sum of two squares iff it is the product of a square and a number that is a sum of two coprime squares. □

Remarks.

- One can classify sums of three squares.
- Other proofs of Corollary 41 are available.

Theorem 42 (Lagrange). Every natural number is a sum of four squares. (Surprising!)

Lecture 14

The Distribution of the Primes

In Lecture 1 we saw Euclid's proof that there are infinitely many primes.

We have results such as:

- There are infinitely many primes congruent to 3 modulo 4 (see examples sheet 1).
- There are infinitely many primes congruent to 1 modulo 4 (see *Numbers & Sets*).

Can we generalise this?

Clearly we cannot show that there are infinitely many primes congruent to 2 modulo 4, or more generally to a modulo n where $(a, n) > 1$. But what happens if $(a, n) = 1$? Are there infinitely many primes congruent to a modulo n?

Things in favour:

- We have some examples.
- All primes lie in $\phi(n)$ residue classes coprime to n (with finitely many exceptions), and there's no obvious reason why one class should be more popular than another.

Theorem 43 (Dirichlet's theorem on primes in arithmetic progressions). Let n be an integer greater than 1, and let a be a natural number coprime to n. Then there are infinitely many primes congruent to a modulo n.

Putting this another way, there are infinitely many primes in the arithmetic progression $a, a + n, a + 2n, a + 3n, \ldots$.

Slogan. "If there is not an obvious reason why there are not infinitely many primes congruent to $a \pmod{n}$, then there are."

Proof. Not proved in this course (so don't use it unless you have to). But we shall see a small hint of an idea of a proof. "□"

We have a successful strategy:

- Want: there are infinitely many primes with some property (e.g., in some congruence class).
- Suppose only finitely many, and aim for contradiction.

- Do something clever to find a number with a prime factor that also has this property.
- Check that this prime is not on the original list – contradiction.

The "something clever" seems to depend heavily upon the property in question, which makes it hard to see how we might use this strategy to prove a more general result.

We need another strategy for showing that there are infinitely many primes. We'll see an approach attributed to Euler, namely to study the sum of reciprocals of primes,

$$\sum_p \frac{1}{p}.$$

How do we expect this to behave?

We know that $\sum 1/n^2$ converges and $\sum 1/n$ diverges. What will happen to $\sum 1/p$?

Proposition 44. For $x \geqslant 10$, we have $\sum_{p \leqslant x} \frac{1}{p} \geqslant \log\log x - \frac{1}{2}$.

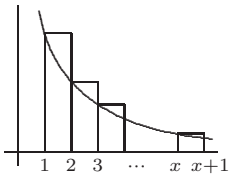
($x \geqslant 10$: only interested in large x; $-\frac{1}{2}$: not important)

Remark. With a bit more work, one can show that $\sum_{p \leqslant x} 1/p = \log\log x + c + O(1/\log x)$ as $x \to \infty$, for some constant c.

So $\sum_{p \leqslant x} 1/p$ diverges, but more slowly than $\sum_{n \leqslant x} 1/n$.

Proof. Idea: look at $\log\left(\prod_{p \leqslant x}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right)\right)$. This includes $\sum_{p \leqslant x} 1/p$, plus other terms which we hope are small. We have:

$$\begin{aligned}
\prod_{p \leqslant x}\left(1 - \frac{1}{p}\right)^{-1} &= \prod_{p \leqslant x}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \\
&\geqslant \sum_{n \leqslant x} \frac{1}{n} \\
&\geqslant \int_1^{x+1} \frac{1}{y}\, dy \\
&\geqslant \log x
\end{aligned}$$



Also we have:

$$\begin{aligned}
\log\left[\left(1 - \frac{1}{p}\right)^{-1}\right] - \frac{1}{p} &= -\log\left(1 - \frac{1}{p}\right) - \frac{1}{p} \\
&= \left(\frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + \cdots\right) - \frac{1}{p} \\
&\leqslant \frac{1}{2p^2} + \frac{1}{2p^3} + \frac{1}{2p^4} + \cdots \\
&= \frac{1/2p^2}{1 - \frac{1}{p}} \\
&= \frac{1}{2p(p-1)}
\end{aligned}$$

Summing over $p \leqslant x$, we have:

$$\begin{aligned}\log\left[\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)^{-1}\right]-\sum_{p\leqslant x}\frac{1}{p} &\leqslant \sum_{p\leqslant x}\frac{1}{2p(p-1)}\\ &\leqslant \sum_{2\leqslant n\leqslant x}\frac{1}{2}\left(\frac{1}{n-1}-\frac{1}{n}\right)\\ &\leqslant \frac{1}{2}\left(1-\frac{1}{x}\right) \leqslant \frac{1}{2}\end{aligned}$$

So

$$\log\log x-\sum_{p\leqslant x}\frac{1}{p} \leqslant \log\left[\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)^{-1}\right]-\sum_{p\leqslant x}\frac{1}{p} \leqslant \frac{1}{2}.$$

So

$$\sum_{p\leqslant x}\frac{1}{p} \geqslant \log\log x-\frac{1}{2}.$$

□

Corollary 45. There are infinitely many primes. □

To prove Dirichlet's theorem, one can show that $\displaystyle\sum_{\substack{p\leqslant x\\ p\equiv a \pmod n}}\frac{1}{p^s}\to\infty$ as $s\to 1$ from above.

One needs a way to pick out primes in this congruence class, and can do this using Dirichlet characters. We shall not say more about this.

We know that all but finitely many primes lie in the $\phi(n)$ residue classes coprime to n. Are they evenly distributed? Look at $\#\{p : p \text{ prime}, p \leqslant x, p \equiv a \pmod n\}$. There are some results and one notable conjecture that is still open (the Elliot-Halberstam conjecture). Roughly speaking, these sets all have approximately the same size.

Let's return to the primes in general, and to $\pi(x)$ which counts the primes $\leqslant x$.

Examples sheet 1: $\pi(x) \geqslant \dfrac{\log x}{2\log\log x}$.

We can get a slightly better bound using an idea of Erdős.

Proposition 46. There is a constant $c > 0$ such that $\pi(x) \geqslant c\log x$.

Proof. If $y \leqslant x$ then we can write $y = m^2 p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, where $m \leqslant \sqrt{x}$, and $p_1,\ldots,p_k$ are the primes $\leqslant x$ (so $k = \pi(x)$), and each α_i is 0 or 1 (so $p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ is square-free).

There are $\leqslant \sqrt{x}$ possibilities for m, and $\leqslant 2^k$ possibilities for $\alpha_1,\ldots,\alpha_k$.

So $x = \#\{y : 1 \leqslant y \leqslant x\} \leqslant \sqrt{x}\,2^{\pi(x)}$.

So $2^{\pi(x)} \geqslant \sqrt{x}$, and so $\pi(x) \geqslant \dfrac{\log x}{2\log 2}$. □

Lecture 15

Definition. We define the **Riemann zeta function** ζ as follows. For a complex number s with $\mathrm{Re}(s) > 1$, we put

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

In this context, one conventionally writes $s = \sigma + it$.

Lemma 47. For $\mathrm{Re}(s) > 1$, the series $\sum_{n=1}^{\infty} 1/n^s$ converges absolutely. Moreover, it converges uniformly on $\mathrm{Re}(s) \geqslant 1 + \delta$ for any $\delta > 0$, and so it is analytic on $\mathrm{Re}(s) > 1$.

Proof. For $s = \sigma + it$ we have: $|n^s| = |n^{\sigma+it}| = \left|e^{(\sigma+it)\log n}\right| = e^{\sigma \log n} = n^{\sigma}$.

So $|1/n^s| = 1/n^{\sigma}$. But $\sum_{n=1}^{\infty} 1/n^{\sigma}$ converges for $\sigma > 1$, and converges uniformly for $\sigma \geqslant 1 + \delta$. □

We can see a link between ζ and prime numbers in the following result.

Proposition 48 (Euler product for ζ). For $\mathrm{Re(s)} > 1$, we have

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

where the product is over all primes.

Proof. Intuitive idea:

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

↑ Fundamental Theorem of Arithmetic

Fix s with $\mathrm{Re}(s) > 1$. If $M > \frac{\log N}{\log 2}$, then $p^M > N$ for any prime p.

So $\prod_{p \leqslant N} \left(\sum_{j=0}^{M} p^{-js} \right)$ equals $1 + 2^{-s} + \cdots N^{-s}$ plus some other terms n^{-s} for $n \geqslant N$.

(Terms are all distinct by the Fundamental Theorem of Arithmetic.)

So

$$\left| \sum_{n=1}^{\infty} n^{-s} - \prod_{p \leqslant N} \left(\sum_{j=0}^{M} p^{-js} \right) \right| \leqslant \sum_{n=N+1}^{\infty} |n^{-s}| = \sum_{n=N+1}^{\infty} n^{-\sigma} \leqslant cN^{1-\sigma},$$

for some constant $c > 0$.

This bound is uniform in M, so taking $M \to \infty$, we get

$$\left| \zeta(s) - \prod_{p \leqslant N} \left(1 - p^{-s}\right)^{-1} \right| \leqslant cN^{1-\sigma}.$$

But $N^{1-\sigma} \to 0$ as $N \to \infty$ (since $\sigma > 1$). So $\zeta(s) = \prod_{p} \left(1 - p^{-s}\right)^{-1}$. □

Remark. This is linked to the study of $\sum_{p \leqslant x} 1/p$ (Proposition 44) where we looked at the product $\prod_{p \leqslant x}(1 - p^{-1})^{-1}$.

It is important to know the location of the zeros of ζ, that is, the values of s for which $\zeta(s) = 0$. We can say something about this now.

Lemma 49. If $\mathrm{Re}(s) > 1$ then $\zeta(s) \neq 0$.

Proof. For $\mathrm{Re}(s) > 1$ we have that $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$. (Clearly each factor is non-zero, but it's an infinite product so we're not sure.)

So $\prod_{p \leqslant x} (1 - p^{-s})^{-1} \neq 0$ for any natural number x.

We have $\zeta(s) \times \prod_{p \leqslant x} (1 - p^{-s}) = \prod_{p > x} (1 - p^{-s})^{-1}$. This is 1 plus the sum of terms n^{-s} where n has a prime factor greater than x.

So $\left| \zeta(s) \times \prod_{p \leqslant x} (1 - p^{-s}) \right| \geqslant 1 - \sum_{n=x+1}^{\infty} n^{-\sigma} \geqslant \frac{1}{2}$ for large enough x.

↖ tail $\to 0$ as $x \to \infty$

So $\zeta(s) = \prod_p (1 - p^{-s})^{-1} \neq 0$. □

It turns out that we can extend ζ to the whole of $\mathbb{C}$ using analytic continuation. One can extend ζ to $\mathrm{Re}(s) > 0$ using an integral. Then ζ turns out to be meromorphic, with a simple pole at $s = 1$.

We define the **Gamma function** to be

$$\Gamma(z) = \int_0^\infty e^{-t} t^{z-1} \, dt, \quad \text{for } \mathrm{Re}(z) > 0$$

This can be continued to a meromorphic function on $\mathbb{C}$ with simple poles at $z = 0, -1, -2, \ldots$ and nowhere else, and with no zeros. The function satisfies $z\Gamma(z) = \Gamma(z-1)$. (So in particular, for a natural number n we have $\Gamma(n) = (n-1)!$.)

We define the **completed ζ function** to be

$$\Xi(s) = \pi^{-s/2} \, \Gamma(s/2) \, \zeta(s)$$

It turns out that Ξ satisfies the functional equation $\Xi(s) = \Xi(1 - s)$.

In this way we can extend ζ to the whole of $\mathbb{C}$. It has just one pole, namely a simple pole at $s = 1$, with residue 1. It has **trivial zeros** at $s = -2, -4, -6, \ldots$. Since $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$, the functional equation tells us that any further zeros of ζ lie in the "critical strip" $0 \leqslant \mathrm{Re}(z) \leqslant 1$.

In order to prove the Prime Number Theorem, mathematicians proved that $\zeta(s) \neq 0$ on the line $\mathrm{Re}(s) = 1$. In fact, we know that there is a zero-region for ζ in the critical strip, and this allows us to prove better error terms in the Prime Number Theorem.

The **Riemann Hypothesis** asserts that in fact all the zeros of ζ in the critical strip lie on the line $\mathrm{Re}(s) = \frac{1}{2}$. (Famous open problem!)

The **Möbius function** $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is defined by

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_1 \ldots p_k \text{ is a product of } k \text{ distinct primes} \\ 0 & \text{if } n \text{ is not square-free} \end{cases}$$

Exercise. Show that μ is multiplicative. (Note $\mu(1) = 1$.)

The **Mertens function** is defined as $\sum_{n\leqslant x}\mu(n)$. The trivial bound is that $\left|\sum_{n\leqslant x}\mu(n)\right|\leqslant x$.

The Riemann Hypothesis is known to be equivalent to the assertion that $\sum_{n\leqslant x}\mu(n) = O_\varepsilon\left(x^{\frac{1}{2}+\varepsilon}\right)$ for all $\varepsilon>0$.

That is, for each $\varepsilon>0$ there is a constant $C_\varepsilon>0$ such that $\left|\sum_{n\leqslant x}\mu(n)\right|\leqslant C_\varepsilon x^{\frac{1}{2}+\varepsilon}$.

Lecture 16

Theorem 50 (Prime Number Theorem). We have $\pi(x)\sim\dfrac{x}{\log x}$.

That is, $\dfrac{\pi(x)}{x/\log x}\to 1$ as $x\to\infty$.

This was first proved in 1896 independently by Hadamard and de la Vallée Poussin. Their argument made use of the Riemann zeta function and complex analysis (Cauchy's Theorem). This left the question of whether there is an "elementary" proof of the theorem. ("Elementary" in the sense of avoiding complex analysis.) This was answered in 1948 when Erdős and Selberg gave an elementary proof – independently, but building on earlier work of Selberg. This is interesting but not substantially easier than previous proofs.

One can prove the Prime Number Theorem with an error term:

Theorem 50′ We have $\pi(x)=\underbrace{\int_2^x\frac{dt}{\log t}}_{\text{logarithmic integral } li(x)} + O\left(xe^{-c\sqrt{\log x}}\right)$ for some constant $c>0$.

It is known that the Riemann Hypothesis is equivalent to: $\pi(x)=\int_2^x\frac{dt}{\log t}+O\left(x^{1/2}\log x\right)$.

How might we study $\pi(x)$? We have

$$\pi(x)=\#\{p:p\leqslant x, p \text{ prime}\}=\sum_{1\leqslant n\leqslant x}\underbrace{1_{\text{prime}}(n)}_{\text{avoids whether } x \text{ is an integer}},$$

where 1_{prime} is the indicator function of the primes,

$$1_{\text{prime}}(n)=\begin{cases}1 & \text{if } n \text{ prime}\\ 0 & \text{otherwise}\end{cases}$$

Using indicator functions in this way can often be helpful. For example, sometimes one can replace an indicator function by its Fourier series.

For this problem, it turns out to be more helpful to work with a weighted indicator function. We want to give more weight to larger (and on average sparser) primes.

Definition. We define the **Von Mangoldt function** Λ as follows. For a natural number, we put

$$\Lambda(n)=\begin{cases}\log p & \text{if } n=p^k \text{ is a prime power}\\ 0 & \text{otherwise}\end{cases}$$

So Λ is a weighted indicator function for primes. There are so few prime powers that their contribution can usually be absorbed into the error term, so we think of Λ as a weighted indicator function of primes.

Instead of studying $\pi(x)=\sum_{1\leqslant n\leqslant x}1_{\text{prime}}(n)$, we study $\psi(x)=\sum_{1\leqslant n\leqslant x}\Lambda(n)$

Often it is easier to work with smoothed indicator functions as this can make issues of convergence easier.

Not  but  or 

One can show that $\pi(x) \sim \dfrac{\psi(x)}{\log x}$, so Theorem 50 is equivalent to the assertion that $\psi(x) \sim x$.

The next result links ζ and Λ.

Lemma 51. If $\mathrm{Re}(s) > 1$ then $\dfrac{\zeta'(s)}{\zeta(s)} = -\displaystyle\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$.

Remarks. $\sum_{n=1}^{\infty} \Lambda(n)/n^s$ is called the **Dirichlet series** for Λ. More generally, is (a_n) is a sequence then we can write a corresponding Dirichlet series $\sum_{n=1}^{\infty} a_n/n^s$.

These turn out to be useful (a sort of generating function).

Proof. Ideas.

- $\frac{\zeta'(s)}{\zeta(s)}$ is the logarithmic derivative of ζ.
- For $\mathrm{Re}(s) > 1$ we have the Euler product for ζ – this is our link between ζ and primes.

For $\mathrm{Re}(s) > 1$, we have $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$. So

$$\log[\zeta(s)] = \log\left[\prod_p \left(1 - p^{-s}\right)^{-1}\right] = -\sum_p \log\left(1 - p^{-s}\right)$$

We want to differentiate both sides with respect to s. Note that $p^{-s} = e^{-s \log p}$, so

$$\frac{d}{ds}(p^{-s}) = -(\log p)\, e^{-s \log p} = -(\log p)\, p^{-s}$$

Therefore

$$\begin{aligned}
\frac{\zeta'(s)}{\zeta(s)} &= -\sum_p \frac{(\log p)\, p^{-s}}{1 - p^{-s}} \\
&= -\sum_p (\log p) p^{-s} \left(1 + p^{-s} + p^{-2s} + \ldots\right) \\
&= -\sum_p \log p \sum_{j=1}^{\infty} p^{-js} \\
&= \sum_n \frac{\Lambda(n)}{n^s}
\end{aligned}$$

□

Using Perron's formula, based on the Mellin transform, one can use this to study ψ. The idea is to integrate $-\frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s}$ along a suitable vertical line in the complex plane. One can use this to deduce an explicit formula for ψ,

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

where the sum is over all zeros ρ of ζ (counting ρ at the same time as $\overline{\rho}$).

So the problem is then to carefully bound the error terms. One important estimate in this is for the number of zeros of ζ.

Let $N(T) = \#\big\{s : \zeta(s) = 0 \text{ and } 0 \leqslant \underset{\nwarrow \mathrm{Re}(s)}{\sigma} \leqslant 1 \text{ and } 0 < \underset{\nwarrow \mathrm{Im}(s)}{t} < T\big\}$.

One can prove that

$$N(T) = \frac{T}{2\pi}\log\left(\frac{T}{2\pi}\right) - \frac{T}{2\pi} + O(\log T)$$

Lecture 17 Try to find $\pi(123) = \#\{p : p \text{ prime}, p \leqslant 123\}$.

- Rule out multiples of 2.
- Rule out multiples of 3.
- Etc.
- Rule out 1.

Every composite number less than 123 has a prime factor $p \leqslant \sqrt{123}$.

Write $P_{11} = \{2, 3, 5, 7, 11\}$, $A_i = \{n : 1 \leqslant n \leqslant 123, i \mid n\}$, and $\overline{A}_i = \{n : 1 \leqslant n \leqslant 123, i \nmid n\}$.

Then

$$\begin{aligned} \pi(123) &= \big|\overline{A}_2 \cap \overline{A}_3 \cap \overline{A}_5 \cap \overline{A}_7 \cap \overline{A}_{11}\big| + \underset{\searrow |P_{11}|}{5} - \underset{\swarrow \text{1 not prime nor composite}}{1} \\ &= 123 - \big|A_2 \cup A_3 \cup A_5 \cup A_7 \cup A_{11}\big| + 4 \end{aligned}$$

By the inclusion-exclusion principle,

$$\big|A_2 \cup A_3 \cup A_5 \cup A_7 \cup A_{11}\big| = \sum_{i \in P_{11}} |A_i| - \sum_{i_1 < i_2} |A_{i_1} \cap A_{i_2}| + \cdots + |A_2 \cap A_3 \cap A_5 \cap A_7 \cap A_{11}|$$

If $i_1, \ldots, i_k$ are distinct, then $|A_{i_1} \cap \ldots \cap A_{i_k}| = |A_{i_1 \ldots i_k}| = \left\lfloor \frac{123}{i_1 \ldots i_k} \right\rfloor$

E.g., $|A_3 \cap A_5 \cap A_7| = |A_{3\times5\times7}| = \left\lfloor \frac{123}{3\times5\times7} \right\rfloor$

Proposition 52 (Legendre's formula). For a real number $x \geqslant 10$, we have

$$\pi(x) = \pi(\sqrt{x}) - 1 + N(x, \sqrt{x}) \qquad \text{(avoid small cases)}$$

where $N(x, \sqrt{x})$ is the number of n with $1 \leqslant n \leqslant x$ and n is not divisible by any prime up to $\sqrt{x}$.

Moreover

$$N(x, \sqrt{x}) = \lfloor x \rfloor - \sum_{i \in P_{\sqrt{x}}} |A_i| + \sum_{\substack{i_1, i_2 \in P_{\sqrt{x}} \\ i_1 < i_2}} |A_{i_1} \cap A_{i_2}| - \cdots + (-1)^{\pi(\sqrt{x})} \Big| \bigcap_{p \in P_{\sqrt{x}}} A_p \Big|$$

where $P_{\sqrt{x}} = \{p : p \text{ prime}, p \leqslant \sqrt{x}\}$ and $A_i = n : 1 \leqslant n \leqslant x, i \mid n\}$.

Proof. A number $n \leqslant x$ is prime iff it is a prime up to $\sqrt{x}$, or it is not divisible by all primes up to $\sqrt{x}$, so $\pi(x) = \pi(\sqrt{x}) - 1 + N(x, \sqrt{x})$.

The formula for $N(x, \sqrt{x})$ follows from $N(x, \sqrt{x}) = \left|\bigcap_{p \in P_{\sqrt{x}}} \overline{A}_p\right|$ and the inclusion-exclusion principle. □

So Legendre's formula allows us to find $\pi(x)$, knowing only primes up to $\sqrt{x}$. Underlying this is the sieve of Eratosthenes. This is perhaps the simplest sieve, and the study of more complicated sieves has led to deep results.

Our next result can be stated in the form of a poem!

> Chebychev said, and I say it again,
> there is always a prime between n and $2n$
>
> – Erdős

This is known as Bertrand's postulate. Erdős gave an elementary proof.

Erdős' idea: if a prime p is between n and $2n$, then it divides the binomial coefficient $\binom{2n}{n}$.

We need a couple of preliminary lemmas.

Lemma 53. For any natural number n, we have $\dfrac{2^{2n}}{2n} \leqslant \dbinom{2n}{n} < 2^{2n}$.

Proof. The upper bound follows from $\binom{2n}{n} < (1+1)^{2n} = 2^{2n}$ (or count subsets of $\{1, \ldots, 2n\}$).

For the lower bound, we use that if $0 \leqslant r \leqslant 2n$ then $\binom{2n}{r} \leqslant \binom{2n}{n}$ and $\binom{2n}{n} \geqslant \binom{2n}{0} + \binom{2n}{2n}$.

So $2^{2n} = (1+1)^{2n} \leqslant 2n\binom{2n}{n}$, giving the lower bound. □

We also want an upper bound on $\prod_{p \leqslant x} p$, the **primorial function**.

Lemma 54. Let x be a real number with $x \geqslant 1$. Then $\displaystyle\prod_{p \leqslant x} p \leqslant 4^x$.

Proof. It suffices to prove when $x = n$ is a natural number, since $\prod_{p \leqslant x} p = \prod_{p \leqslant \lfloor x \rfloor} p$.

Use induction on n: case $n = 2$ is clear.

Induction step. Suppose the result holds for values up to n, where $n \geqslant 2$.

- If n is odd, then $n+1$ is not prime, so by the induction hypothesis,

$$\prod_{p \leqslant n+1} p \;=\; \prod_{p \leqslant n} p \;\leqslant\; 4^n \;<\; 4^{n+1}$$

- If n is even, then $n = 2k$ for some $k \in \mathbb{N}$. We have

$$\prod_{p \leqslant 2k+1} p \;=\; \left(\prod_{p \leqslant k+1} p\right) \times \left(\prod_{k+2 \leqslant p \leqslant 2k+1} p\right) \;\leqslant\; 4^{k+1}\left(\prod_{k+2 \leqslant p \leqslant 2k+1} p\right)$$

by the induction hypothesis.

The product $\prod_{k+2 \leqslant p \leqslant 2k+1} p$ divides the binomial coefficient $\binom{2k+1}{k+1}$, since

$$\binom{2k+1}{k+1} = \frac{(2k+1)(2k)\cdots(k+2)}{k!}$$

and each prime in $[k+2, 2k+1]$ divides the numerator and is coprime to the denominator.

But $2\binom{2k+1}{k+1} = \binom{2k+1}{k} + \binom{2k+1}{k+1} \leqslant \sum_{i=0}^{2k+1} \binom{2k+1}{i} = 2^{2k+1}$.

So $\prod_{k+2 \leqslant p \leqslant 2k+1} p \leqslant \binom{2k+1}{k+1} \leqslant 2^{2k} = 4^k$.

So $\prod_{p \leqslant 2k+1} p \leqslant 4^{k+1} \cdot 4^k = 4^{2k+1}$. □

Theorem 55 (Bertrand's postulate). Let n be a natural number. Then there is a prime p with $n < p \leqslant 2n$. (Equality for case $n = 1$.)

Proof. Consider $\binom{2n}{n}$. We want $\prod_{n<p\leqslant 2n} p > 1$.

For a natural number N and a prime p, write $\alpha(p, N)$ for the exponent of p in the prime factorisation of $N!$, so

$$\alpha(p, N) = \left\lfloor \frac{N}{p} \right\rfloor + \left\lfloor \frac{N}{p^2} \right\rfloor + \dots$$

(See examples sheet 3, question 6.)

Then we have

$$\binom{2n}{n} = \left(\prod_{n<p\leqslant 2n} p \right) \times \left(\prod_{p \leqslant n} p^{\alpha(p,2n) - 2\alpha(p,n)} \right)$$

since $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$

Write $\alpha(p) = \alpha(p, 2n) - 2\alpha(p, n)$, so $\alpha(p) = \sum_{j=1}^{\infty} \left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor \right)$.

If $p^j > 2n$, then the summand $\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor = 0$. So each summand is 0 or 1.

So $\alpha(p) \leqslant \sum_{1 \leqslant j \leqslant \frac{\log(2n)}{\log p}} 1 \leqslant \frac{\log(2n)}{\log p}$, so $p^{\alpha(p)} \leqslant 2n$.

We shall use this for small p, but can do better for larger p.

If $p^2 > 2n$, then $\alpha(p) = \left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor$ is 0 or 1.

So we split the product further: write $\binom{2n}{n} = T_1 T_2 T_3$, where

$$
\begin{aligned}
T_1 &= \prod_{p \leqslant \sqrt{2n}} p^{\alpha(p)} \leqslant (2n)^{\pi(\sqrt{2n})} \\
T_2 &= \prod_{\sqrt{2n} < p \leqslant n} p^{\alpha(p)} \leqslant \prod_{\sqrt{2n} < p \leqslant n} p \\
T_3 &= \prod_{n < p \leqslant 2n} p
\end{aligned}
$$

Lecture 18

So,

$$
T_3 = \binom{2n}{n} \times \frac{1}{T_1} \times \frac{1}{T_2} \geqslant \frac{2^{2n}}{2n} \times \frac{1}{(2n)^{\pi(\sqrt{2n})}} \times \frac{1}{T_2}
$$

We have $T_2 \leqslant \prod_{\sqrt{2n} < p \leqslant n} p \leqslant 4^n$ (by Lemma 54), but this is not strong enough.

If $\frac{n}{2} < p \leqslant n$, then p appears just once in $n!$ (because $2p$ is too large). So if we can ensure that p appears exactly twice in $(2n)!$, then we'll have $\alpha(p) = 0$. So we want $3p > 2n$, i.e. $p > \frac{2n}{3}$.

So if $p > \frac{2n}{3}$, then $\alpha(p) = 0$, and so $T_2 \leqslant \prod_{\sqrt{2n} < p \leqslant \frac{2n}{3}} \leqslant 4^{2n/3}$, by Lemma 54.

So $T_3 = \prod_{n < p \leqslant 2n} p \geqslant \frac{2^{2n}}{2n} \times \frac{1}{(2n)^{\pi(\sqrt{2n})}} \times 4^{-2n/3} \geqslant \frac{4^{n/3}}{(2n)^{1+\pi(\sqrt{2n})}}$ ← want this > 1

We want an upper bound on $1 + \pi(\sqrt{2n})$. But $1 + \pi(\sqrt{2n}) < \frac{1}{2}\sqrt{2n}$, as even numbers greater than 2 are not prime, and 9 and 15 are not prime.

So $T_3 > \frac{2^{2n/3}}{(2n)^{\frac{1}{2}\sqrt{2n}}} = \left(\frac{2^{\sqrt{2n}}}{(\sqrt{2n})^3} \right)^{\sqrt{2n}/3}$.

For integers $m \geqslant 12$ we have $2^{m-1} \geqslant m^3$ (easy induction), so for $x \geqslant 12$ we have $2^x \geqslant x^3$.

So for $n \geqslant 100$ we have $\frac{2^{\sqrt{2n}}}{(\sqrt{2n})^3} \geqslant 1$, and so $T_3 > 1$.

The result is easy to check for the remaining values of n. □

Continued Fractions

If we take an irrational (e.g., $\sqrt{2}$), how can we approximate it by a rational number? We could find the decimal expansion and chop it off at some point. (This certainly gives a rational approximation – but is it the *best* rational approximation?)

We'd like a rational with a small denominator that is very close to the original number.

Proposition 56 (Dirichlet). Let θ (usually irrational) be a real number, and let N be a natural number. Then there is a rational a/q with $1 \leqslant q \leqslant N$, such that $|\theta - a/q| \leqslant 1/qN$. ($q$: small denominator)

Proof. Idea: look at $0, \theta, 2\theta, \ldots, N\theta$ and use pigeonhole principle.

We consider $r\theta$, where $0 \leqslant r \leqslant N$, working modulo 1.

Divide the unit interval/circle into intervals $\left[\frac{j}{N}, \frac{j+1}{N}\right]$ of length $1/N$. Then we have $N+1$ values of $r\theta$, lying in N intervals.

So by the pigeonhole principle there are two values in the same interval, say corresponding to $r\theta$ and $s\theta$, where $r < s$.

But then $(s-r)\theta$ is within $1/N$ of an integer. So if $q = s - r$ then $|q\theta - a| < 1/N$ for some integer a and $1 \leqslant q \leqslant N$. □

Continued fractions will give us a way to study Diophantine approximation in more detail.

Example. Like division in Euclid's algorithm: $67 = 2 \times 24 + 19 \Rightarrow \frac{67}{24} = 2 + \frac{19}{24}$.

$$\left.\begin{array}{rcl} \frac{67}{24} & = & 2 + \frac{19}{24} \\ \frac{24}{19} & = & 1 + \frac{5}{19} \\ \frac{19}{5} & = & 3 + \frac{4}{5} \\ \frac{5}{4} & = & 1 + \frac{1}{4} \\ \frac{4}{1} & = & 4 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl} \frac{67}{24} & = & 2 + \frac{1}{24/19} \\ & = & 2 + \frac{1}{1+\frac{1}{19/5}} \\ & = & \cdots \\ & = & 2 + \frac{1}{1+\frac{1}{3+\frac{1}{1+\frac{1}{4}}}} \end{array}\right.$$

The last expression is a continued fraction for $\frac{67}{24}$. We put $a_0 = \left\lfloor \frac{67}{24} \right\rfloor$, then picked α_1 such that $\frac{67}{24} = a_0 + \frac{1}{\alpha_1}$, then put $a_1 = \lfloor \alpha_1 \rfloor$ and repeated.

Definition. A **continued fraction** is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

where a_0 is an integer and $a_1, a_2, \ldots$ are natural numbers. We also write this as $[a_0, a_1, a_2, \ldots]$. The a_i are called **partial quotients**.

The continued fraction may stop, e.g. $[a_0, \ldots, a_n]$, in which case we call it **finite**. Or it may continue forever, in which case we call it **infinite**.

If $[a_0, a_1, \ldots, a_n]$ is a finite continued fraction then we impose the condition $a_n > 1$ (because we could replace a_{n-1} by $a_{n-1} + 1$). I.e., $\frac{1}{a_{n-1}+\frac{1}{1}} = \frac{1}{a_{n-1}+1}$.

It will be convenient to allow a_n in $[a_0, a_1, \ldots, a_n]$ to be something other than a natural number.

Lemma 57. There is a one-one correspondence between finite continued fractions and rational numbers. (final denominator > 1)

Proof. Clearly a finite continued fraction is a rational number (just multiply up).

Let θ be a rational number. We must put $a_0 = \lfloor \theta \rfloor$, since $0 < \dfrac{1}{[a_1, \ldots, a_n]} < 1$.

We pick α_1 such that $\theta = a_0 + \dfrac{1}{\alpha_1}$, so put $\alpha_1 = \dfrac{1}{\theta - a_0}$.

Then α_1 is a rational, with denominator strictly less than that of θ.

Then we must pick $a_1 = \lfloor \alpha_1 \rfloor$ and so recursively define $\alpha_{i+1} = \dfrac{1}{\alpha_i - a_i}$ for $i \geqslant 0$.
So $\alpha_i = a_i + \frac{1}{\alpha_{i+1}}$.

Then the α_i form a sequence of rational numbers with strictly decreasing denominators. So the process must stop – at some point we have $a_n = \alpha_n$. (Exactly the same argument as for Euclid's algorithm.)

So we have a finite continued fraction. □

Lecture 19

Definition. Let $[a_0, a_1, \ldots]$ be a continued fraction. Then the finite continued fractions $[a_0]$, $[a_0, a_1]$, $[a_0, a_1, a_2]$, ... are called the **convergents** for $[a_0, a_1, \ldots]$.

Example.

$$\begin{aligned}
[a_0] &= a_0 \\
[a_0, a_1] &= a_0 + \tfrac{1}{a_1} = \tfrac{a_0 a_1 + 1}{a_1} \\
[a_0, a_1, a_2] &= a_0 + \tfrac{1}{a_1 + \frac{1}{a_2}} = a_0 + \tfrac{a_2}{a_1 a_2 + 1} = \tfrac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1} \\
[a_0, a_1, a_2, a_3] &= \left[a_0, a_1, a_2 + \tfrac{1}{a_3}\right] = \tfrac{a_0 a_1 \left(a_2 + \frac{1}{a_3}\right) + a_0 + \left(a_2 + \frac{1}{a_3}\right)}{a_1 \left(a_2 + \frac{1}{a_3}\right) + 1} \\
&= \tfrac{a_0 a_1 a_2 a_3 + a_0 a_1 + a_0 a_3 + a_2 a_3 + 1}{a_1 a_2 a_3 + a_1 + a_3}
\end{aligned}$$

Definition. We define two sequences (p_n) and (q_n), given $a_0, a_1, \ldots$ real numbers with $a_1, a_2, \ldots \geqslant 1$.

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

($\frac{p_n}{q_n}$ will be convergents.)

Lemma 58. For $n \geqslant 0$, we have $\dfrac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$.

Proof. By induction on n.

$n = 0$: $\dfrac{p_0}{q_0} = \dfrac{a_0}{1} = [a_0]$.

$n = 1$: $\dfrac{p_1}{q_1} = \dfrac{a_0 a_1 + 1}{a_1} = a_0 + \dfrac{1}{a_1} = [a_0, a_1]$.

Suppose the results hold for n, where $n \geqslant 1$. Then

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

□

Here is a useful fact about the convergents.

Lemma 59. For $n \geqslant 1$, we have $p_n q_{n-1} - p_{n-1}q_n = (-1)^{n+1}$. So $\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n+1}}{q_{n-1}q_n}$.

Proof. By induction on n. For $n = 1$: $p_1q_0 - p_0q_1 = (a_0a_1 + 1) - a_0a_1 = 1 = (-1)^2$.

Induction step. Suppose true for $n \geqslant 1$, then

$$\begin{aligned}
p_{n+1}q_n - p_nq_{n+1} &= (a_{n+1}p_n + p_{n-1})q_n - p_n(a_{n+1}q_n + q_{n-1}) \\
&= a_{n+1}p_nq_n + p_{n-1}q_n - p_nq_na_{n+1} - p_nq_{n-1} \\
&= -(p_nq_{n-1} - p_{n-1}q_n) \\
&= (-1)^{n+2} \quad \text{by induction hypothesis}
\end{aligned}$$

□

One immediate consequence:

Lemma 60. If $a_0, a_1, \ldots, a_n$ are integers, then p_n and q_n are coprime integers.

Proof. For $n = 0$, we have $(p_0, q_0) = (a_0, 1) = 1$.

For $n \geqslant 1$, if $d \mid p_n$ and $d \mid q_n$ then $d \mid (p_nq_{n-1} - p_{n-1}q_n)$, so $d \mid 1$, so $(p_n, q_n) = 1$. □

So $\dfrac{p_n}{q_n}$ is a rational in lowest terms.

We saw before that there is only one continued fraction for a given rational number. If an irrational number θ has a continued fraction, then it will have to be obtained in the same way:

$$a_0 = \lfloor \theta \rfloor, \quad \alpha_1 = \frac{1}{\theta - a_0}$$

$$\text{and for } i \geqslant 1, \quad a_i = \lfloor \alpha_i \rfloor, \quad \alpha_{i+1} = \frac{1}{\alpha_i - a_i}$$

Example. Let $\theta = \sqrt{3}$.

$$\begin{aligned}
a_0 &= \lfloor \theta \rfloor = 1 \\
\alpha_1 &= \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} \\
a_1 &= \lfloor \alpha_1 \rfloor = 1 \\
\alpha_2 &= \frac{1}{\frac{\sqrt{3}+1}{2}-1} = \frac{2}{\sqrt{3}-1} = \frac{2(\sqrt{3}+1)}{2} = \sqrt{3}+1 \\
a_2 &= \lfloor \alpha_2 \rfloor = 2 \\
\alpha_3 &= \frac{1}{(\sqrt{3}+1)-2} = \frac{1}{\sqrt{3}-1} = \alpha_1 \text{ so keep repeating}
\end{aligned}$$

So if $\sqrt{3}$ has a continued fraction then it would be $[1, 1, 2, 1, 2, \ldots]$, written $[1; \overline{1, 2}]$.

What are the convergents? Use the recurrences:

$$\frac{1}{1}, \frac{2}{1}, \frac{5}{3}, \frac{7}{4}, \frac{19}{11}, \frac{26}{15}, \ldots \longleftrightarrow 1,\ 2,\ 1.66,\ 1.75,\ 1.7272\ldots,\ 1.7333\ldots,\ \ldots$$

Compare $\sqrt{3} = 1.7320\ldots$, so perhaps the convergents $\to \sqrt{3}$?

Proposition 61. Let θ be an irrational number, and define a_i, p_i, q_i as above. Then $\dfrac{p_n}{q_n} \to \theta$ as $n \to \infty$.

Remark. This makes sense of infinite continued fractions. We define $[a_0, a_1, \ldots]$ to be the limit of $[a_0]$, $[a_0, a_1]$, $[a_0, a_1, a_2]$, $\ldots$

Proof. We have $\theta = [a_0, a_1, \ldots, a_n, \alpha_{n+1}]$, by our definitions of a_i and α_{n+1}.

This equals $\dfrac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}$ by Lemma 58. (Useful.)

Then

$$\begin{aligned}
\left|\theta - \frac{p_n}{q_n}\right| &= \left|\frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n}\right| \\
&= \left|\frac{q_n\alpha_{n+1}p_n + q_np_{n-1} - p_n\alpha_{n+1}q_n - p_nq_{n-1}}{q_n(\alpha_{n+1}q_n + q_{n-1})}\right| \\
&= \left|\frac{p_{n-1}q_n - p_nq_{n-1}}{q_n(\alpha_{n+1}q_n + q_{n-1})}\right| \\
&= \left|\frac{(-1)^n}{q_n(\alpha_{n+1}q_n + q_{n-1})}\right| \quad \text{(by Lemma 59)}
\end{aligned}$$

The q_n form a sequence of strictly increasing natural numbers (by the recurrence relation), so $q_n \to \infty$ as $n \to \infty$.

Hence $\left|\theta - \dfrac{p_n}{q_n}\right| \to 0$ as $n \to \infty$. □

Lemma 62. We have $\dfrac{1}{q_{n+2}} \leqslant |q_n\theta - p_n| \leqslant \dfrac{1}{q_{n+1}}$.

Moreover, for $n \geqslant 1$, we have $|q_n\theta - p_n| \leqslant |q_{n-1}\theta - p_{n-1}|$.

Proof. As in the proof of Proposition 61, we have $|q_n\theta - p_n| = \dfrac{1}{\alpha_{n+1}q_n + q_{n-1}}$.

We have $a_{n+1} \leqslant \alpha_{n+1} \leqslant a_{n+1} + 1$,

$$\begin{aligned} \text{so} \quad \alpha_{n+1}q_n + q_{n-1} &\geqslant a_{n+1}q_n + q_{n-1} \\ &= q_{n+1} \\ \text{and} \quad \alpha_{n+1}q_n + q_{n-1} &\leqslant (a_{n+1}+1)q_n + q_{n-1} \\ &= (a_{n+1}q_n + q_{n-1}) + q_n \\ &= q_{n+1} + q_n \\ &\leqslant a_{n+2}q_{n+1} + q_n \\ &= q_{n+2} \end{aligned}$$

So $\dfrac{1}{q_{n+2}} \leqslant |q_n\theta - p_n| \leqslant \dfrac{1}{q_{n+1}}$.

It follows immediately that $|q_n\theta - p_n| \leqslant |q_{n-1}\theta - p_{n-1}|$. □

Lecture 20

Throughout this lecture, θ is an irrational with convergents $\dfrac{p_n}{q_n}$.

Theorem 63. Let n be a natural number. If p and q are integers with $0 < q < q_n$, then $|q\theta - p| \geqslant |q_{n-1}\theta - p_{n-1}|$.

Remark. Amongst all rationals with denominator $< q_n$, the "best rational approximation" is $\dfrac{p_{n-1}}{q_{n-1}}$.

Proof. Idea. Write p and q in terms of convergents.

The matrix $\begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix}$ has determinant $p_{n-1}q_n - p_nq_{n-1} = (-1)^n$, by Lemma 59.

So the matrix is invertible and its inverse has integer entries.

So $\begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix}^{-1} \begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}$ for some integers u, v.

So $\left.\begin{array}{l} p = up_{n-1} + vp_n \\ q = uq_{n-1} + vq_n \end{array}\right\}$ for some integers u, v.

Now, $|q\theta - p| \;=\; |uq_{n-1}\theta + vq_n\theta - up_{n-1} - vp_n| \;=\; |u(q_{n-1}\theta - p_{n-1}) + v(q_n\theta - p_n)|$.

We have $0 < q < q_n$, so $0 < uq_{n-1} + vq_n < q_n$, so $u \neq 0$, and u, v have opposite signs.

Also, $\theta - \dfrac{p_{n-1}}{q_{n-1}}$ and $\theta - \dfrac{p_n}{q_n}$ have opposite signs (using the expression for this quantity in the proof of Proposition 61).

So $u(q_{n-1}\theta - p_{n-1})$ and $v(q_n\theta - p_n)$ have the same sign.

So $|q\theta - p| \;=\; |u(q_{n-1}\theta - p_{n-1})| + |v(q_n\theta - p_n)| \;\geqslant\; |q_{n-1}\theta - p_{n-1}|$. □

important and useful

Corollary 64. If p is an integer and q is a natural number with $\left|\theta - \frac{p}{q}\right| < \frac{1}{2q^2}$, then $\frac{p}{q}$ is a convergent for θ.

Proof. We may assume that p and q are coprime.

Pick n such that $q_n \leqslant q < q_{n+1}$. (Guess that $\frac{p}{q} = \frac{p_n}{q_n}$.)

Then $\left|\frac{p}{q} - \frac{p_n}{q_n}\right| \leqslant \left|\frac{p}{q} - \theta\right| + \left|\frac{p_n}{q_n} - \theta\right| < \frac{1}{2q^2} + \frac{1}{q_n}|q_n\theta - p_n|$.

But by Theorem 63 we have $|q_n\theta - p_n| \leqslant |q\theta - p|$.

So $\left|\frac{p}{q} - \frac{p_n}{q_n}\right| < \frac{1}{2q^2} + \frac{1}{q_n}|q\theta - p| < \frac{1}{2qq_n} + \frac{1}{q_n}\frac{1}{2q} = \frac{1}{qq_n}$.

But we also have $\left|\frac{p}{q} - \frac{p_n}{q_n}\right| = \frac{|pq_n - p_nq|}{qq_n}$, so $|pq_n - p_nq| < 1$.

But $pq_n - p_nq$ is an integer, so $pq_n - p_nq = 0$. □

We are going to study the **Diophantine equation** $x^2 - Ny^2 = 1$, where N is a fixed natural number that is not a square. This is called **Pell's equation**. This equation arises when looking for units in certain quadratic number fields – see the *Number Fields* course.

Corollary 65. Let N be a natural number that is not a square. If x, y are positive integers such that $x^2 - Ny^2 = 1$, then x/y is a convergent for $\sqrt{N}$.

exclude $y=0$

"If Pell's equation has any solutions, they are amongst the convergents for $\sqrt{N}$."

Proof. We have $x^2 - Ny^2 = 1$, so $(x - y\sqrt{N})(x + y\sqrt{N}) = 1$.

So $x - y\sqrt{N} > 0$, and $x - y\sqrt{N} = \frac{1}{x + y\sqrt{N}} < \frac{1}{2y\sqrt{N}} < \frac{1}{2y}$.

So $\left|\frac{x}{y} - \sqrt{N}\right| < \frac{1}{2y^2}$, so by Corollary 64, $\frac{x}{y}$ is a convergent for $\sqrt{N}$. □

We saw previously that the continued fraction for $\sqrt{3}$ is eventually periodic.

Definition. A continued fraction is **eventually periodic** if it is of the form

$$\left[a_0, a_1, \ldots, a_{n-1}; \overline{a_n, \ldots, a_{n+m-1}}\right].$$

It is **purely periodic** if of the form $\left[\overline{a_0, a_1, \ldots, a_{m-1}}\right]$.

Definition. The real number θ is a **quadratic irrational** if $a\theta^2 + b\theta + c = 0$ for some integers a, b, c, with $a \neq 0$.

Theorem 66 (Lagrange). The real number θ is a quadratic irrational if and only if its continued fraction is eventually periodic.

Sketch Proof (see a book for details).

($\Leftarrow$). If $\theta = \left[a_0, a_1, \ldots, a_{n-1}, \overline{a_n, \ldots, a_{n+m-1}}\right]$, then let $\phi = \left[\overline{a_n, \ldots, a_{n+m-1}}\right]$, so then $\phi = [a_n, \ldots, a_{n+m-1}, \phi]$.

So $\phi = \dfrac{\phi\, p'_{m-1} + p'_{m-2}}{\phi\, q'_{m-1} + q'_{m-2}}$, where $\dfrac{p'_{m-1}}{q'_{m-1}}$ and $\dfrac{p'_{m-2}}{q'_{m-2}}$ are convergents for ϕ.

So ϕ is a quadratic irrational.

Also $\theta = [a_0, a_1, \ldots, a_{n-1}, \phi] = \dfrac{\phi\, p_{n-1} + p_{n-2}}{\phi\, q_{n-1} + q_{n-2}}$ is also a quadratic irrational.

($\Rightarrow$). We have $a\theta^2 + b\theta + c = 0$, say. So $f(\theta, 1) = 0$ for the binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$.

Idea: show that there are only finitely many possibilities for α_n.

Do this by showing that there are only finitely many values of $f(p_n, q_n)$. □

One can say more about the continued fraction for $\sqrt{N}$. (Recall $\sqrt{3} = [1; \overline{1, 2}]$.)

Theorem 67. The continued fraction for $\sqrt{N}$ is of the form $\left[a_0; \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}\right]$.

Proof. Omitted.

We can use this to find a solution to Pell's equation.

Proposition 68. Let N be a natural number that is not a square. Then there is a convergent $\dfrac{p_n}{q_n}$ for $\sqrt{N}$ with $p_n^2 - Nq_n^2 = 1$.

Proof. We have

$$\sqrt{N} \;=\; \left[a_0; \overline{a_1, \ldots, a_n, 2a_0}\right] \;=\; \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}},$$

where $\alpha_{n+1} = \left[\overline{2a_0, a_1, \ldots, a_n}\right] = a_0 + \sqrt{N}$.

So $\sqrt{N} = \dfrac{(a_0 + \sqrt{N})p_n + p_{n-1}}{(a_0 + \sqrt{N})q_n + q_{n-1}}$.

$\implies a_0 q_n \sqrt{N} + q_n N + q_{n-1}\sqrt{N} = a_0 p_n + p_n \sqrt{N} + p_{n-1}$.

$\implies \sqrt{N}(a_0 q_n + q_{n-1} - p_n) = a_0 p_n + p_{n-1} - q_n N$.

But $\sqrt{N}$ is irrational, so: $\left.\begin{array}{l} a_0 q_n + q_{n-1} - p_n = 0 \\ a_0 p_n + p_{n-1} - q_n N = 0 \end{array}\right\} \implies \left\{\begin{array}{l} p_{n-1} = q_n N - a_0 p_n \\ q_{n-1} = p_n - a_0 q_n \end{array}\right.$.

But $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$, by Lemma 59.

So $p_n(p_n - a_0 q_n) - (q_n N - a_0 p_n) q_n = (-1)^{n+1}$, so $p_n^2 - N q_n^2 = (-1)^{n+1}$.

If n is odd, then we have a solution: (p_n, q_n).

If n is even, then the same argument applied to the convergents at the next period shows that (p_{2n+1}, q_{2n+1}) is a solution. □

Lecture 21

Example. Find a solution to $x^2 - 14y^2 = 1$.

Start by finding the continued fraction for $\sqrt{14}$.

$$\begin{aligned}
a_0 &= \lfloor \sqrt{14} \rfloor = 3 \\
\alpha_1 &= \frac{1}{\sqrt{14}-3} = \frac{\sqrt{14}+3}{5} \implies a_1 = 1 \\
\alpha_2 &= \frac{1}{\frac{\sqrt{14}+3}{5}-1} = \frac{5}{\sqrt{14}-2} = \frac{\sqrt{14}+2}{2} \implies a_2 = 2 \\
\alpha_3 &= \frac{1}{\frac{\sqrt{14}+2}{2}-2} = \frac{2}{\sqrt{14}-2} \implies a_3 = 1 \\
\alpha_4 &= \frac{1}{\frac{\sqrt{14}+2}{5}-1} = \frac{5}{\sqrt{14}-3} = \sqrt{14}+3 \implies a_4 = 6
\end{aligned}$$

So $\sqrt{14} = [3; \overbrace{1, 2, 1}^{\text{symmetric}}, \overbrace{6}^{2a_0}]$.

We saw in Proposition 68 that we should look at $\frac{p_3}{q_3}$. Use recurrences:

$$\begin{aligned}
p_0 = 3, \quad p_1 = 4, \quad p_2 = 11, \quad p_3 = 15 \\
q_0 = 1, \quad q_1 = 1, \quad q_2 = 3, \quad q_3 = 4
\end{aligned}$$

It's easy to check that $15^2 - 14 \times 4^2 = 225 - 224 = 1$, so $x = 15$, $y = 4$ is indeed a solution.

We can find a second solution from $[3, 1, 2, 1; \overline{6, 1, 2, 1}]$.

$$\begin{aligned}
p_4 = 101, \quad p_5 = 116, \quad p_6 = 333, \quad p_7 = 449 \\
q_4 = 27, \quad q_5 = 31, \quad q_6 = 89, \quad q_7 = 120
\end{aligned}$$

And $x = 449$, $y = 120$ is a solution.

There is some useful structure to the solutions of $x^2 - Ny^2 = 1$.

Lemma 69. If (x_1, y_1) and (x_2, y_2) are solutions to $x^2 - Ny^2 = 1$, then so is

$$(x_1x_2 + y_1y_2N\,,\; x_1y_2 + x_2y_1).$$

Proof. Note that

$$(x_1 \pm y_1\sqrt{N})(x_2 \pm y_2\sqrt{N}) = x_1x_2 + y_1y_2N \pm (x_1y_2 + x_2y_1)\sqrt{N}$$

(same sign)

If we knew about norms in a suitable number field, the result follows.

We have

$$\begin{aligned}
&(x_1x_2 + y_1y_2N)^2 - N(x_1y_2 + x_2y_1)^2 \\
&\quad = \left[(x_1x_2 + y_1y_2N) - (x_1y_2 + x_2y_1)\sqrt{N}\right]\left[(x_1x_2 + y_1y_2N) + (x_1y_2 + x_2y_1)\sqrt{N}\right] \\
&\quad = (x_1 - y_1\sqrt{N})(x_2 - y_2\sqrt{N})(x_1 + y_1\sqrt{N})(x_2 + y_2\sqrt{N}) \\
&\quad = (x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2)
\end{aligned}$$

□

Example (continued). We had the solution $(x_1, y_1) = (15, 4)$.

So $(x_1^2 + 14y_1^2,\ 2x_1y_1) = (225 + 224,\ 2 \times 15 \times 4) = (449, 120)$ is also a solution.

Remark. If we define an operation $*$ by $(x_1, y_1) * (x_2, y_2) = (x_1x_2 + y_1y_2N, x_1y_2 + x_2y_1)$, then the solutions to $x^2 - Ny^2 = 1$ form a group under $*$. Moreover, this group is cyclic, generated by a **fundamental unit** which comes from continued fractions as in the proof of Proposition 68. In particular, there are infinitely many solutions to Pell's equation. See "Dirichlet's unit theorem" in *Number Fields*.

Primality Testing and Factorisation

We have two key questions in the section:

- Given a large integer N, can we efficiently determine if N is prime?
- Given a large composite integer N, can we efficiently find a prime factor of N?

For the first question, dividing N by all primes up to $\sqrt{N}$ is *not* efficient.

We know that if p is prime then $a^{p-1} \equiv 1 \pmod{p}$ for all a coprime to p (Fermat's Little Theorem). Does this give a primality test?

E.g., $n = 15$. We have $2^{14} \equiv 2^{4\times3+2} \equiv 2^2 \equiv 4 \pmod{15}$ and $(2, 15) = 1$, so 15 is not prime.

Definition. Let n be an odd composite natural number and let b be coprime to n. We say that n is a **(Fermat) pseudoprime to the base** b if $b^{n-1} \equiv 1 \pmod{n}$.
So n behaves like a prime as far as b is concerned.

E.g., 15 is a pseudoprime to base 4.

If n is not pseudoprime to some base b then it is not prime – if it is then we cannot tell.

Lemma 70. If n is a pseudoprime to bases b_1 and b_2, then n is also a pseudoprime to bases b_1b_2 and $b_1b_2^{-1}$. (Subgroup.)

Proof. We have $b_1^{n-1} \equiv b_2^{n-1} \equiv 1 \pmod{n}$, so $(b_1b_2)^{n-1} \equiv (b_1b_2^{-1})^{n-1} \equiv 1 \pmod{n}$.

(And clearly b_1b_2 and $b_1b_2^{-1}$ are each coprime to n). □

Proposition 71. Suppose that n is not pseudoprime to some base b. Then for at least half of all bases, n is not pseudoprime.

Proof. Idea. Want #bases to which not pseudoprime $\geqslant$ #bases to which pseudoprime – so for each base to which n is pseudoprime, find another to which it is not.

We know that n is not pseudoprime to the base b. Let B be the set of all bases to which n is pseudoprime.

Define $f : B \to \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \setminus B$ by $b_1 \mapsto bb_1$.

This makes sense, since if n is pseudoprime to the base b_1, then by Lemma 70 it is not pseudoprime to the base bb_1. Since f is an injection, we are done. □

This is a good strategy. It can be phrased more algebraically – proper subgroups have index at least 2.

So for a primality test, pick a few bases and see whether n is pseudoprime to them. Could we have a composite n that is pseudoprime to every base? Unfortunately, yes!

Definition. The odd composite natural number n is called a **Carmichael number** if it is a pseudoprime to every base.

(See examples sheet 4 for more information and examples.)

It turns out that there are infinitely many Carmichael numbers. This was proved in the early 1990s by Alford, Granville and Pomerance.

We know that if p is prime and a is coprime to p, then $a^{p-1} \equiv 1 \pmod{p}$, so $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. (The only square roots of 1 (mod p) are ± 1.) In fact, we know more. Euler's criterion says that $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Definition. Let n be an odd composite natural number and let b be coprime to n. We say that n is an **Euler pseudoprime to base** b if $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$.

Jacobi symbol

Lecture 22

Lemma 72. If n not an Euler pseudoprime to some base b, then for at least half of all possible bases we find n is not an Euler pseudoprime.

Proof. Mimic proofs of Lemma 70 and Proposition 71.

Suppose that n is an Euler pseudoprime to the bases b_1 and b_2. Then $(b_1 b_2)^{\frac{n-1}{2}} \equiv \left(\frac{b_1}{n}\right)\left(\frac{b_2}{n}\right) \equiv \left(\frac{b_1 b_2}{n}\right) \pmod{n}$.

So n is also an Euler pseudoprime to the base $b_1 b_2$, and similarly for $b_1 b_2^{-1}$.

Let B be the set of all bases to which n is an Euler pseudoprime. Then define $f : B \to \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \setminus B$ by $b_1 \mapsto b b_1$.

This is well-defined and an injection. (Same proof as for Fermat pseudoprimes.) □

Examples.

- $n = 15$, $b = 4$.
  Then $4^7 \equiv (4^2)^3 \times 4 \equiv 4 \pmod{15}$, so $4^7 \not\equiv \left(\frac{4}{15}\right) \pmod{15}$.
  So 15 is not an Euler pseudoprime to the base 4. (So 15 must be composite.)
- $n = 15$, $b = 14$.
  Then $14^7 \equiv (-1)^7 \equiv -1 \pmod{15}$ and $\left(\frac{14}{15}\right) = \left(\frac{14}{3}\right)\left(\frac{14}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = -1$.
  So 15 is an Euler pseudoprime to the base 14.

Remark. If n is an Euler pseudoprime to the base b, then $b^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$, so $b^{n-1} \equiv 1 \pmod{n}$, so n is a Fermat pseudoprime to the base b, but the converse is not true.

It turns out that there are not analogues of Carmichael numbers for the notion of Euler pseudoprimes.

Proposition 73. Let n be an odd composite natural number. Then n is an Euler pseudoprime to at most half of all possible bases.
(Very different from the case of Fermat pseudoprimes.)

Proof. By Lemma 72, it suffices to show that there is a base b to which n is not an Euler pseudoprime. We split into two cases.

- n is divisible by the square of a prime (odd)

  Claim. There is b such that $b^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}$.

  (And so certainly $b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) \pmod{n}$.)

  Proof. We have $p^2 \mid n$ for some prime p.

  If $b^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$, then $b^{n-1} \equiv 1 \pmod{n}$, so $b^{n-1} \equiv 1 \pmod{p^2}$. So the order of b modulo p^2 divides $n-1$.

  Working modulo p^2 is good, because we know that $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times$ is cyclic. Take g as a generator modulo p^2, so g has order $p(p-1)$ modulo p^2.

  Consider $b = g^{p-1}$. This has order p modulo p^2. But $p \nmid n-1$, so $b^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{p}$.

- n is a product of distinct primes

  Claim. There is some b such that $\left(\frac{b}{n}\right) = -1$ but $b^{\frac{n-1}{2}} \not\equiv -1 \pmod{n}$, then done.

  Proof. Let p be a prime dividing n. Then there is λ such that $\left(\frac{\lambda}{p}\right) = -1$.

  Pick b such that: $b \equiv \lambda \pmod{p}$
  $b \equiv 1 \pmod{\frac{n}{p}}$

  (Possible by Chinese remainder theorem, since p and $\frac{n}{p}$ coprime.)

  Then $b^{\frac{n-1}{2}} \not\equiv -1 \pmod{\frac{n}{p}}$, so $b^{\frac{n-1}{2}} \not\equiv -1 \pmod{n}$.

  But $\left(\frac{b}{n}\right) = \left(\frac{b}{p}\right) \times 1 = -1$. □

This gives us the idea for the **Solovay-Strassen primality test**.

1. Pick n.
2. Choose some random bases.
3. Check whether n is an Euler pseudoprime to each of those bases.

   If n is not an Euler pseudoprime to one of those bases, then stop – n is composite.

   If n is an Euler pseudoprime to k different bases, then the probability that it is composite is at most $1/2^k$.

This is a **probabilistic primality test**, but very useful.

If p is prime and a is coprime to p, then $a^{p-1} \equiv 1 \pmod{p}$, so $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.

If $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and $\frac{p-1}{2}$ is even, then we could do the same again: $a^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}$.

And so on. This motivates the following definition.

Definition. Let n be an odd composite natural number and let b be coprime to n. Write $n - 1 = 2^s t$ where $s \geqslant 1$ and t is odd.

We say that n is a **strong pseudoprime to the base** b if $b^t \equiv 1 \pmod{n}$ or $b^{2^r t} \equiv -1 \pmod{n}$ for some r with $0 \leqslant r \leqslant s - 1$.

(This would hold if n were prime.)

Example.

- $n = 65$, $b = 8$.

  Then $n - 1 = 2^6$ so take $s = 6$, $t = 1$.

  Have $b^1 = 8 \not\equiv \pm 1 \pmod{65}$, but $b^2 = 8^2 \equiv -1 \pmod{65}$.

  So 65 is a strong pseudoprime to the base 8.

- $n = 65$, $b = 2$.

  Then $b^1 \equiv 2^1 \not\equiv \pm 1 \pmod{65}$
  $b^2 \equiv 2^2 \not\equiv \pm 1 \pmod{65}$
  $b^4 \equiv 2^4 \not\equiv \pm 1 \pmod{65}$
  $b^8 \equiv 2^8 \not\equiv \pm 1 \pmod{65}$
  $b^{16} \equiv 2^{16} \not\equiv \pm 1 \pmod{65}$
  $b^{32} \equiv 2^{32} \not\equiv -1 \pmod{65}$

If n is not a strong pseudoprime to some base b, then n is composite.

Proposition 74. If n is a strong pseudoprime to the base b, then it is also an Euler pseudoprime to the base b.

Proof. Omitted. (See *Koblitz*, for example.)

Is there an analogue of Proposition 73 for strong pseudoprimes?

Theorem 75. Let n be an odd composite natural number. Then n is a strong pseudoprime to at most one quarter of all possible bases.

Proof. Omitted. (See *Koblitz*, for example.)

This leads to the **Miller-Rabin primality test**. Pick n, find s, t such that $n - 1 = 2^s t$, where t odd.

1. Choose a random base b.

2. Compute $b^t \pmod n$. If it is ± 1 then return to step 1.

3. Compute $b^{2t}, b^{4t}, \ldots, b^{2^{s-1}t} \pmod n$ (by repeated squaring).

   If $b^{2^r t} \equiv -1 \pmod n$ for some r then stop and return to step 1.

4. If we reach step 4, then n is not a strong pseudoprime to the base b, so n is composite.

   Otherwise, if n is a strong pseudoprime to k different bases, then n is composite with probability at most $1/4^k$.

There are other primality tests, including **deterministic tests** (rather than probabilistic). See *Koblitz* or *Davenport*.

One in particular is the Agrawal-Kayal-Saxena test (AKS test) announced in 2002. Four key features:

- works on any natural number n
- it is deterministic
- its running time is polynomial in the number of digits of n
- it does not rely on any unproved conjectures (some tests rely on the Generalised Riemann Hypothesis, for example)

Lecture 23

Factorisation

Throughout this section, N will be a large odd composite natural number that is not a square. We want to find a, b such that $N = ab$ and $1 < b < a$. Note that a, b are both odd, so $r = \frac{1}{2}(a+b)$ and $s = \frac{1}{2}(a-b)$ are both integers.

Also, $N = ab = (r-s)(r+s) = r^2 - s^2$. So there is a correspondence between factorisations and differences of two squares. So if we can find r, s such that $N = r^2 - s^2$, then we obtain a factorisation.

Idea. Try values of r such that $r^2 - N$ is a small positive number and check whether it's a square.

This is the idea behind **Fermat factorisation**.

- Pick $r = \lfloor \sqrt{N} \rfloor + 1, \lfloor \sqrt{N} \rfloor + 2, \ldots$.
- For each value of r, test to see whether $r^2 - N$ is a perfect square. If so, call it s^2.
- Then $N = r^2 - s^2$, so $r - s$ and $r + s$ are factors of N.

Example. $N = 200819$.

Try $r = \lfloor \sqrt{200819} \rfloor + 1 = 449$. Then $r^2 - N = 449^2 - 200819 = 782$. (Not a square.)

Try $r = \lfloor \sqrt{200819} \rfloor + 2 = 450$. Then $r^2 - N = 450^2 - 200819 = 1681 = 41^2$.

So $200819 = (450 - 41)(450 + 41) = 409 \times 491$.

This example worked with a few steps because $N = 200819$ has factors close to $\sqrt{N}$. In general, the method is guaranteed to find a proper factor, but it might take a while. (See examples sheet 4.)

We can adapt this slightly, by trying $r = \lfloor\sqrt{kN}\rfloor + 1, \lfloor\sqrt{kN}\rfloor + 2, \ldots$, for small natural numbers k. If $r^2 - kN$ is a square, say $kN = r^2 - s^2$, then N divides $(r-s)(r+s)$. We can then compute the highest common factor of N and $r - s$ and hope that this is a non-trival factor of N (although it might not be). Perhaps try a few values of r, then change k and try a few more values of r, and so on.

More generally, if we have r, s for which $r^2 \equiv s^2 \pmod{N}$ then $N \mid (r-s)(r+s)$, and so we can hope to find a non-trivial factor of N by computing $(N, r-s)$ or $(N, r+s)$. (Finding hcf can be done efficiently by Euclid's algorithm.)

How might we find such r and s? Trying values of r and hoping $r^2 - N$ is a square is a bit optimistic. Instead, we could look for several values of r such that r^2 is congruent to something small modulo N. Then these "small numbers" will be products of a few small primes, and so hopefully some will multiply to give a square.

Definition. Recall (from section on Gauss' Lemma) we write $\langle b \rangle$ for the residue congruent to b modulo n lying in $\left(-\frac{N}{2}, \frac{N}{2}\right)$. We call this the **least absolute residue** of b.

Definition. A **factor base** B is a set of a few small primes, together with -1.

Say that b is a B**-number** if $\langle b^2 \rangle$ is a product of elements from B (repetition allowed).

We have the **factor base method**.

1. Choose a suitable factor base B.
2. Choose some B-numbers $b_1, \ldots, b_k$.
3. Find some $I \subseteq \{1, \ldots, k\}$ such that $\prod_{i \in I} \langle b_i^2 \rangle$ is a square.
4. Let $c^2 = \prod_{i \in I} \langle b_i^2 \rangle$, let $b = \prod_{i \in I} b_i$. Then $b^2 \equiv c^2 \pmod{N}$.
5. Compute $(N, b-c)$ or $(N, b+c)$ and hope that if gives a non-trivial factor of N. If not, try some more B-numbers.

Warning. It is not necessarily the case that $N = (N, b-c)(N, b+c)$.

E.g., $N = 105$, $b = 25$, $c = 10$. Then $105 \mid (25-10)(25+10)$, but $(105, 25-10) = 15$, $(105, 25+10) = 35$, and $105 \neq 15 \times 35$.

Steps 3 and 5 can be carried out efficiently by a computer. Step 5 is just Euclid's algorithm. Step 3 can be thought of as follows.

Let $B = \{p_1, \ldots, p_r\}$. For each $\langle b_i^2 \rangle$ there is an r-tuple $(\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,r}) \in \mathbb{F}_2^r$, where

$$\alpha_{i,j} = \left\{ \begin{matrix} 0 \\ 1 \end{matrix} \right\} \text{ if the exponent of } p_j \text{ in the prime factorisation of } \langle b_i^2 \rangle \text{ is } \left\{ \begin{matrix} \text{even} \\ \text{odd} \end{matrix} \right\}.$$

($\mathbb{F}_2$ is the field with 2 elements. $\mathbb{F}_2^r$ is an r-dimensional vector space over $\mathbb{F}_2$.)

Then we want $I \subseteq \{1, \ldots, k\}$ such that $\sum_{i \in I} (\alpha_{i,1}, \ldots, \alpha_{i,r}) \equiv (0, \ldots, 0) \pmod{2}$.

So we want a linear dependence among vectors in $\mathbb{F}_2^r$. Note that $\mathbb{F}_2^r$ is an r-dimensional vector space, so if $k \geqslant r+1$ then we are guaranteed to have such a dependence. (But often we can get away with fewer.)

Example. $N = 1829$.

Factor base, $B = \{-1, 2, 3, 5, 7, 11, 13, 17, 19\}$. (Just choose small primes.)

B-numbers: try $\lfloor\sqrt{1829k}\rfloor$, $\lfloor\sqrt{1829k}\rfloor + 1$, for $k = 1, 2, 3, \ldots$. (When we compute $\langle b_i^2 \rangle$, we should get something small.)

b_i	42	43	60	61	74	75	85
$\langle b_i^2 \rangle$	-65	20	-58	63	-11	138	-91
factorisation	$-1 \cdot 5 \cdot 13$	$2^2 \cdot 5$	$-1 \cdot 2 \cdot 29$	$3^2 \cdot 7$	$-1 \cdot 11$	$2 \cdot 3 \cdot 23$	$-1 \cdot 7 \cdot 13$
B-number?	yes	yes	no	yes	yes	no	yes

(Keep testing as you go along.)

So $(42 \times 43 \times 61 \times 85)^2 \equiv (-1)^2 \times 2^2 \times 3^2 \times 5^2 \times 7^2 \times 13^2 \pmod{1829}$.

We have $42 \times 43 \times 61 \times 85 \equiv 1459 \pmod{1859}$, so put $b = 1459$.

And $(-1) \times 2 \times 3 \times 5 \times 7 \times 13 \equiv -901 \pmod{1859}$, so put $c = -901$.

Then $(N, b + c) = (1829, 1459 - 901) = (1929, 558) = 31$, so get $1829 = 31 \times 59$.

Lecture 24

How does one choose good B-numbers?

We want numbers b such that $\langle b^2 \rangle$ is a product of small prime powers, so look for b such that $\langle b^2 \rangle$ is small. One approach is to use $\lfloor\sqrt{kN}\rfloor$ and $\lfloor\sqrt{kN}\rfloor + 1$ (as in the example above).

Another approach uses continued fractions.

Idea. If $\frac{p_n}{q_n}$ is a convergent for $\sqrt{N}$, then p_n is close to $q_n\sqrt{N}$, so p_n^2 is close to $q_n^2 N$. So perhaps $p_n^2 - q_n^2 N$ is $\langle p_n^2 \rangle$, and perhaps it is small enough that the p_n will be good B-numbers.

Lemma 76. Let $\dfrac{p_n}{q_n}$ be a convergent for $\sqrt{N}$.

Then $\langle p_n^2 \rangle = p_n^2 - q_n^2 N$, and moreover $|\langle p_n^2 \rangle| \leqslant 2\sqrt{N}$. $\longleftarrow$ smaller than $\frac{1}{2}N$

Proof. Since $\dfrac{p_n}{q_n}$ is a convergent for $\sqrt{N}$, by Lemma 62 we have $|p_n - q_n\sqrt{N}| \leqslant \dfrac{1}{q_{n+1}}$.

Also,

$$\begin{aligned} p_n + q_n\sqrt{N} &\leqslant |p_n - q_n\sqrt{N}| + q_n\sqrt{N} + q_n\sqrt{N} \\ &\leqslant \frac{1}{q_{n+1}} + 2q_n\sqrt{N} \end{aligned}$$

So

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

So $p_n^2 - q_n^2 N \equiv p_n^2 \pmod{N}$ and $p_n^2 - q_n^2 N \in \left(-\frac{N}{2}, \frac{N}{2}\right)$.

So $\langle p_n^2 \rangle = p_n^2 - q_n^2 N$ and $|\langle p_n^2 \rangle| \leqslant 2\sqrt{N}$. □

This gives the idea for the **continued fraction method**, which is a variant of the factor base method.

A. Compute the first few partial quotients a_i in the continued fraction for $\sqrt{N}$.

B. Compute the first few numerators of convergents p_n using the recurrence

$$\left.\begin{array}{l} p_0 = a_0 \\ p_1 = a_0 a_1 + 1 \\ p_k = a_k p_{k-1} + p_{k-2} \quad \text{for } k \geqslant 2 \end{array}\right\} \text{working mod } p \text{ throughout.}$$

C. Compute $\langle p_n^2 \rangle$ and factorise.

D. Choose factor base B to include -1, any primes that occur to an even power in the factorisation of a $\langle p_n^2 \rangle$ and any primes that occur to an odd power in the factorisation of at least two $\langle p_n^2 \rangle$.

Note which of the $\langle p_n^2 \rangle$ are then B-numbers.

E. Then continue from Step 3 in the factor base method.

Example. $N = 12403$.

a_i	111	2	1	2	2	7	1	
p_i	111	223	334	891	2116	3300	5416	← reduce mod 12403
$\langle p_i^2 \rangle$	-82	117	-71	89	-27	166	-39	
fact'n	$-1 \cdot 2 \cdot 41$	$\underline{3^2 \cdot 13}$	$-1 \cdot 71$	89	$\underline{-1 \cdot 3^3}$	$2 \cdot 83$	$\underline{-1 \cdot 3 \cdot 13}$	

(Fill in a few terms of the a_i row first. Then fill in columns, always looking for a useful factorisation.)

So $(223 \times 2116 \times 5416)^2 \equiv ((-1) \times 3^3 \times 13)^2 \pmod{12403}$.

We have $223 \times 2116 \times 5416 \equiv 11341 \pmod{12403}$, so put $b = 11341$.

And $(-1) \times 3^3 \times 13 = -351$, so put $c = -351$.

Then $(N, b + c) = (12403, 10990) = 157$, so get $12403 = 157 \times 79$.

Note. As with the factor base method, if $(N, b \pm c)$ is not a proper factor of N, then compute some more B-numbers (in this case numerators of convergents) and try again.

One more factorisation method.

Idea. If p is a prime factor of N, then $p \mid N$ and $p \mid a^{p-1} - 1$ for any a coprime to p, so $p \mid (N, a^{p-1} - 1)$. But we can't compute $(N, a^{p-1} - 1)$ because we can't compute $a^{p-1} - 1$, because we don't know p.

We know that $p - 1$ is even, and hopefully it is a product of a few small prime powers. If so, and if k is a product of *lots* of small prime powers, then $p - 1 \mid k$. But then $a^k \equiv 1 \pmod{p}$, so $(N, a^k - 1)$ is hopefully a proper factor of N.

This is the idea behind **Pollard's $p - 1$ method**.

1. Choose k that is a product of lots of small prime powers.
   (E.g., $k = B!$, or $k = \mathrm{lcm}(1, 2, \ldots, B)$, for some B.)
2. Choose a coprime to N.
   (E.g., small value like 2 or 3, or choose a at random.)
3. Compute a^k modulo N.
   (E.g., by repeated squaring: find $a, a^2, a^4, a^8, \ldots$ modulo N and then assemble a suitable product.)
4. Compute $(N, a^k - 1)$ and hope it is a proper factor of N.

If this fails, it might be because $N \mid a^k - 1$, in which case choose another value of k. Or it might be that if p is a prime dividing N, then $p - 1$ does not divide this k, so choose a larger k and try again. It is possible that every prime p dividing N is such that $p - 1$ has a large prime factor, in which case one needs an adaptation of this. See *Koblitz* or *Davenport*, for example.

Example. $N = 540143$.

Try $B = 8$, put $k = \mathrm{lcm}(1, 2, \ldots, 8) = 2^3 \times 3 \times 5 \times 7 = 840$.

Try $a = 2$. We have $2^{840} \equiv 53047 \pmod{540143}$.

Then $(540143, \underbrace{53047 - 1}_{a^k - 1}) = 421$, and we get $540143 = 421 \times 1283$.

There is currently no known classical method for factorising large numbers very efficiently. But if one has a quantum computer then one can factorise a large number very efficiently (the time take is polynomial in $\log N$), thanks for Shor's algorithm. But that's another story.

Number Theory — Examples Sheet 1

Michaelmas Term 2011 *V. Neale*

Notation: for a real number x, we write $\lfloor x \rfloor$ for the *floor function* of x. That is, $\lfloor x \rfloor$ is the largest integer less than or equal to x.

1. Calculate $d = (a, b)$ and find integers x and y such that $d = ax + by$ when

   (i) $a = 841$, $b = 160$;

   (ii) $a = 2613$, $b = 2171$.

2. Let a and b be integers with $a > b > 1$. Let $\lambda(a, b)$ denote the number of individual applications of Euclid's algorithm required to compute the highest common factor of a and b.

   (i) Find a pair of four-digit numbers a and b for which $\lambda(a, b)$ is very small.

   (ii) Find a pair of four-digit numbers a and b for which $\lambda(a, b)$ is large.

   (iii) Prove that
   $$\lambda(a, b) \leqslant 2 \left\lfloor \frac{\log b}{\log 2} \right\rfloor .$$

3. This question is about Diophantine equations of the form $ax + by = c$, where a, b and c are fixed natural numbers and we are interested in integer solutions (x, y). Where possible, give an example of such an equation that has

   (i) no solutions;

   (ii) exactly one solution;

   (iii) infinitely many solutions;

   and briefly justify your answers.

4. Let x be an integer greater than 1. Use the Fundamental Theorem of Arithmetic to show that
   $$x \leqslant \left(1 + \frac{\log x}{\log 2}\right)^{\pi(x)} .$$
   Deduce that when $x \geqslant 8$ we have $\pi(x) \geqslant \frac{\log x}{2 \log \log x}$.

5. Let a and n be integers greater than 1. Prove that if $a^n - 1$ is prime, then $a = 2$ and n is prime. Is the converse true?

6. Let q be an odd prime. Prove that every prime factor of $2^q - 1$ must be congruent to 1 mod q, and also congruent to ± 1 mod 8. Use this to factor $2^{11} - 1 = 2047$.

7. We say that a natural number n is *perfect* if the sum of all the positive divisors of n is equal to $2n$. Prove that a positive even integer n is perfect if and only if it can be written in the form $n = 2^{q-1}(2^q - 1)$, where $2^q - 1$ is prime.

   (It is conjectured that there are no odd perfect numbers, but this is as yet unknown.)

8. By considering numbers of the form $n = 2^2 \cdot 3 \cdot 5 \cdot \cdots \cdot p - 1$, prove that there are infinitely many primes congruent to 3 mod 4.

9. Find the smallest non-negative integer x satisfying the congruences $x \equiv 2 (\mathrm{mod}\, 3)$, $x \equiv 3 (\mathrm{mod}\, 5)$, $x \equiv 4 (\mathrm{mod}\, 11)$, $x \equiv 5 (\mathrm{mod}\, 16)$.

10. Find all integers x satisfying both $19x \equiv 103 (\mathrm{mod}\, 900)$ and $10x \equiv 511 (\mathrm{mod}\, 841)$.

11. A positive integer is said to be *square-free* if it is the product of distinct primes. (So 174 is square-free but 175 is not, for example.) Are there 100 consecutive numbers that are *not* square-free?

12. Prove that the classes of both 2 and 3 generate $(\mathbb{Z}/5^n\mathbb{Z})^\times$ for all positive integers n. For each of the primes $p = 11$, 13, 17 and 19, find a generator of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for all $n \geqslant 1$.

13. Let A be the group $(\mathbb{Z}/65520\mathbb{Z})^\times$. Determine the least positive integer n such that $g^n = 1$ for all g in A.

14. Let a and n be integers greater than 1, and put $N = a^n - 1$. Show that the order of $a + N\mathbb{Z}$ in $(\mathbb{Z}/N\mathbb{Z})^\times$ is exactly n, and deduce that n divides $\phi(N)$. If n is a prime, deduce that there are infinitely many primes q such that $q \equiv 1 (\mathrm{mod}\, n)$.

Please e-mail me with comments, suggestions and queries (v.r.neale@dpmms.cam.ac.uk).

Number Theory — Examples Sheet 2

Michaelmas Term 2011 *V. Neale*

1. Evaluate the following Jacobi symbols (in fact, they are Legendre symbols): $\left(\frac{20964}{1987}\right)$, $\left(\frac{741}{9283}\right)$, $\left(\frac{5}{160465489}\right)$, $\left(\frac{3083}{3911}\right)$.

2. Find all odd primes p for which 15 is a quadratic residue modulo p.

3. Prove that 3 is a quadratic non-residue modulo any Mersenne prime $2^n - 1$, with $n > 2$.

4. Let p be a prime with $p \equiv 1 (\mathrm{mod}\, 4)$. Prove that the sum of the quadratic residues in the interval $[1, p-1]$ is equal to the sum of the quadratic non-residues in this interval. Does this hold if $p \equiv 3 (\mathrm{mod}\, 4)$?

5. Let a be a positive integer that is not a square. Prove that there are infinitely many odd primes p such that $\left(\frac{a}{p}\right) = -1$.

6. Are the forms $3x^2 + 2xy + 23y^2$ and $2x^2 + 4xy + 5y^2$ equivalent (under the action of $SL_2(\mathbb{Z})$)? Are the forms $15x^2 - 15xy + 4y^2$ and $3x^2 + 9xy + 8y^2$ equivalent?

7. Prove that equivalence of binary quadratic forms is an equivalence relation.

8. Make a list of all reduced positive definite quadratic forms of discriminant $-d$, where $d = 8$, 11, 12, 16, 19, 23, 163.

9. Find the smallest positive integer that can be represented by the form $4x^2 + 17xy + 20y^2$.

10. Find a necessary and sufficient condition for a prime p to be represented by the form $x^2 + 3y^2$.

11. Is there a positive definite binary quadratic form that represents 2 and the primes congruent to 1 (mod 8) or 3 (mod 8), but no other primes?

12. Find a necessary and sufficient condition for a positive integer n to be properly represented by at least one of the two forms $x^2 + xy + 4y^2$ and $2x^2 + xy + 2y^2$.

    Assume that n is coprime to 15, and properly represented by at least one of the forms. Show that congruence conditions modulo 15 allow one to decide which form represents n.

Please e-mail me with comments, suggestions and queries (v.r.neale@dpmms.cam.ac.uk).

Number Theory — Examples Sheet 3

Michaelmas Term 2011 *V. Neale*

Throughout this sheet, ϕ denotes the Euler totient function, μ the Möbius function, $d(n)$ the number of positive divisors of n, and $\sigma(n)$ the sum of the positive divisors of n.

1. Prove that for $\Re(s) > 1$, we have

$$\zeta^2(s) = \sum_{n=1}^{\infty} \frac{d(n)}{n^s}.$$

   Can you find Dirichlet series for $1/\zeta(s)$ and $\zeta(s-1)/\zeta(s)$ (for suitable values of s)?

2. Find all natural numbers n for which $\sigma(n) + \phi(n) = nd(n)$.

3. (i) Compute $\sum_{d|n} \mu(d)$ for natural numbers n.

   (ii) Let f be a function defined on the natural numbers, and define g by $g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$. Find an expression for f in terms of g.

   (iii) Find a relationship between μ and ϕ.

4. Compute $\sum_{d|n} \Lambda(d)$ for natural numbers n. (Here Λ is the von Mangoldt function.)

5. Use Legendre's formula to compute $\pi(207)$.

6. Let N be a positive integer greater than 1.

   (i) Show that the exact power of a prime p dividing $N!$ is $\sum_{k=1}^{\infty} \lfloor \frac{N}{p^k} \rfloor$.

   (ii) Prove the inequality $N! > (\frac{N}{e})^N$.

   (iii) Deduce that

$$\sum_{p \leqslant N} \frac{\log p}{p-1} > \log N - 1.$$

7. Prove that every non-constant polynomial with integer coefficients assumes infinitely many composite values.

8. Prove that every integer $N > 6$ can be expressed as a sum of distinct primes.

9. Calculate a_0, ..., a_4 in the continued fraction expansions of e and π.

10. Let a be a positive integer. Determine explicitly the real number whose continued fraction is $[a, a, a, \dots]$.

11. Determine the continued fraction expansions of $\sqrt{3}$, $\sqrt{7}$, $\sqrt{13}$, $\sqrt{19}$, $\sqrt{46}$.

Please e-mail me with comments, suggestions and queries (v.r.neale@dpmms.cam.ac.uk).

Number Theory — Examples Sheet 4

Michaelmas Term 2011 *V. Neale*

1. Let N and M be positive integers such that N is not a square and such that $M \leqslant \sqrt{N}$. Prove that if x and y are positive integers satisfying $x^2 - Ny^2 = M$ then x/y is a convergent of $\sqrt{N}$.

2. Determine which of the equations $x^2 - 31y^2 = 1$, $x^2 - 31y^2 = 4$ and $x^2 - 31y^2 = 5$ are soluble in positive integers x and y. For each that is soluble, exhibit at least one solution.

3. Find two solutions in positive integers x and y of the equation $x^2 - Ny^2 = 1$ when $N = 3$, 7, 13, 19, 46.

4. Find all bases for which 39 is an Euler pseudoprime.

5. Let n be an odd composite integer.

   (i) Show that if n is a Carmichael number, then n is square-free.

   (ii) Show that n is a Carmichael number if and only if $p - 1 | n - 1$ for every prime p dividing n.

   (iii) Show that if n is a Carmichael number, then n is the product of at least three distinct primes.

   (iv) Find the smallest Carmichael number.

6. Let $N = (6t+1)(12t+1)(18t+1)$, where t is a positive integer such that $6t+1$, $12t+1$ and $18t+1$ are all prime numbers. Prove that N is a Carmichael number. Use this construction to find three Carmichael numbers.

7. Prove that there are 36 bases for which 91 is a pseudoprime. More generally, show that if p and $2p-1$ are both prime numbers, then $N = p(2p-1)$ is a pseudoprime for precisely half of all bases.

8. Let $N = 561$. Find the number of bases b for which N is an Euler pseudoprime. Show that there are precisely 10 bases for which N is a strong pseudoprime.

9. Let p be a prime greater than 5. Prove that $N = (4^p + 1)/5$ is a composite integer. Prove that N is a strong pseudoprime to the base 2.

10. Assume that n is an integer greater than 1 such that $F_n = 2^{2^n} + 1$ is composite ($n = 5$, ...). Prove that F_n is a pseudoprime to the base 2.

11. Prove that if N has a factor which is within $\sqrt[4]{N}$ of $\sqrt{N}$, then Fermat factorisation must work on the first try.

12. Use Fermat factorisation to factorise the integers 8633, 809009, and 92296873.

13. Explain why when we use the continued fraction algorithm for factorising N, there is no need to include in the factor base B any prime with $\left(\frac{N}{p}\right) = -1$.

14. Let $N = 2701$. Use the B-numbers 52 and 53 for a suitable factor base B to factor 2701.

15. Use Pollard's $p-1$ method with $k = 840$ and $a = 2$ to try to factorise $N = 54367$. Then try with $a = 3$.

16. Use the continued fraction algorithm to factorise the integers 9509, 13561, 8777 and 14429.

Please e-mail me with comments, suggestions and queries (v.r.neale@dpmms.cam.ac.uk).