

# Part II - Number Theory

Lectured by Prof. T. A. Fisher

Artur Avameri

Lent 2022

## Contents

<b>0</b>	<b>Introduction</b>	<b>2</b>
<b>1</b>	<b>Euclid's algorithm and factoring</b>	<b>3</b>
<b>2</b>	<b>Congruences</b>	<b>5</b>
2.1	Polynomial congruences . . . . .	9
<b>3</b>	<b>Quadratic residues</b>	<b>12</b>
<b>4</b>	<b>Binary quadratic forms</b>	<b>19</b>

## 0 Introduction

06 Oct 2022,  
Lecture 1

Books:

- A. Baker, *A concise introduction to the theory of numbers*, CUP 1984
- N. Koblitz, *A course in number theory & cryptography*, Springer 1994
- H. Davenport, *The higher arithmetic*, CUP 2008

Number theory studies the hidden and mysterious properties of the integers and the rational numbers.

It has always been an experimental science. Examining numerical data leads to **conjectures**, many of which are very old and still unproven today.

**Example 0.1.** (i) Let  $N \geq 1$  be an integer of the form  $8n + 5, 8n + 6$  or  $8n + 7$ . Does there exist a right-angled triangle of area  $N$ , all of whose sides have rational length? We don't know.

(ii) Let  $\pi(x)$  be the number of primes less than or equal to  $x$  and define  $\text{li}(x) = \int_2^x \frac{dt}{\log t}$ . Then for all  $x \geq 3$ ,  $|\pi(x) - \text{li}(x)| \leq \sqrt{x} \log x$ . This is in fact equivalent to the Riemann hypothesis.

(iii) There are infinitely many twin primes. We now know there is an integer  $N \leq 246$  such that there are infinitely many pairs of primes the form  $p, p + N$ .

## 1 Euclid's algorithm and factoring

**Definition 1.1** (Division algorithm). Given  $a, b \in \mathbb{Z}$ , with  $b > 0$ , there exist  $q, r \in \mathbb{Z}$  such that  $a = qb + r$ , and  $0 \leq r < b$ .

**Notation.** If  $r = 0$ , then we write  $b|a$ , else  $b \nmid a$ .

*Proof.* Let  $S = \{a - nb \mid n \in \mathbb{Z}\}$ . This certainly contains integers  $\geq 0$ , so take the smallest one  $r$ . We claim  $r < b$ . Indeed, if not, then  $r - b \geq 0$ , contradicting minimality.  $\square$

Given  $a_1, \dots, a_n \in \mathbb{Z}$  not all zero, let  $I = \{\lambda_1 a_1 + \dots + \lambda_n a_n \mid \lambda_i \in \mathbb{Z}\}$ .

**Lemma 1.1.**  $I = d\mathbb{Z}$  for some  $d > 0$ .

*Proof.*  $I$  certainly contains integers  $\geq 0$ . Let  $d$  be the least positive element of  $I$ . We claim it works. Take  $a \in I$ , then  $a = qd + r$  with  $0 \leq r < d$ . But  $r = a - qd \in I \implies r = 0$ .  $\square$

**Remark.** We get from this that  $d$  divides each  $a_i$ , and any common divisor of the  $a_i$  must divide  $d$ . Why?

We write  $d = \gcd(a_1, \dots, a_n)$  for the **greatest common divisor** (or **highest common factor**), or just use the shorthand  $d = (a_1, \dots, a_n)$ .

**Corollary 1.2.** Let  $a, b, c \in \mathbb{Z}$ . Then there exist  $x, y \in \mathbb{Z}$  such that  $ax + by = c$  if and only if  $(a, b) | c$ .

The division algorithm gives a very efficient way to compute  $(a, b)$ . Assume  $a > b > 0$ . Apply the division algorithm recursively to get

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

**Claim.**  $r_k = (a, b)$ . Indeed,  $(a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{k-1}, r_k) = r_k$ . This is called **Euclid's algorithm**.

**Remark.** If  $d = (a, b)$ , then by Lemma 1.2, there exist  $r, s \in \mathbb{Z}$  such that  $ra + sb = d$ . Euclid's algorithm gives us a way to find  $r$  and  $s$ .

In the following table,  $x$  and  $y$  stand for 34 and 25, and we then compute remainders as linear combinations of them.

We can use a trick here to speed this up: find each row as  $q \cdot$  the row before it + the second row before it, then figure out signs at the end. (In fact, the minus signs zigzag down).

$$\begin{array}{r|rr}
 & x & y \\
 a = 34 & 1 & 0 \\
 b = 25 & 0 & 1 \\
 34 = 1 \cdot 25 + 9 & 1 & -1 \\
 25 = 2 \cdot 9 + 7 & -2 & 3 \\
 9 = 1 \cdot 7 + 2 & 3 & -4 \\
 7 = 3 \cdot 2 + 1 & -11 & 15
 \end{array}$$

We hence get  $-11 \cdot 34 + 15 \cdot 25 = 1$ .

**Definition 1.2.** An integer  $n > 1$  is **prime** if its only positive divisors are 1 and  $n$ . Otherwise  $n$  is **composite**.

**Lemma 1.3.** Let  $p$  be a prime, and  $a, b \in \mathbb{Z}$ . If  $p|ab$ , then  $p|a$  or  $p|b$ .

*Proof.* Assume  $p \nmid a$ . Then  $(a, p) = 1$ . By Lemma 1.2,  $\exists r, s \in \mathbb{Z}$  such that  $ra + sp = 1 \implies rab + spb = b$ . Since  $p|ab$ ,  $p|b$  follows.  $\square$

**Theorem 1.4 (Fundamental Theorem of Arithmetic).** Every integer  $n > 1$  can be written as a product of primes. This representation is unique up to reordering.

*Proof.* Existence is obvious. For uniqueness, suppose  $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$  for  $p_i, q_i$  primes. We have  $p_1 | q_1 q_2 \dots q_r$ , so by Lemma 1.5,  $p_1 | q_j$  for some  $j$ , so  $p_1 = q_j$ . Now cancel these out and induct.  $\square$

**Remark.** If  $m = \prod_{i=1}^k p_i^{\alpha_i}$  and  $n = \prod_{i=1}^k p_i^{\beta_i}$  for  $p_i$  distinct primes and  $\alpha_i, \beta_i \geq 0$ , then

$$(m, n) = \prod_{i=1}^k p_i^{\min(\alpha_i, \beta_i)}.$$

However, if  $m$  and  $n$  are large, it is more efficient to compute  $(m, n)$  using Euclid's algorithm.

Suppose we have some large positive integer  $N$ . An obvious algorithm for factoring  $N$  is to trial divide by 2 and the odd integers up to  $\sqrt{N}$ .

**Definition 1.3.** An algorithm with input a positive integer  $N$  is **polynomial** or a **polynomial time** algorithm if it takes  $\leq c(\log N)^b$  **elementary operations** for some constants  $b$  and  $c$ .

**Remark.** An elementary operation is just adding/multiplying two numbers in  $\{0, 1, \dots, 9\}$ .

08 Oct 2022,  
Lecture 2

**Remark.** "Polynomial" makes sense here as it takes  $\log N$  digits to write  $N$ .

Polynomial algorithms are known for:

- Adding and multiplying integers (the usual way);
- Computing gcd's (via Euclid's algorithm);
- Detecting  $n^{\text{th}}$  powers (compute  $\sqrt[n]{\phantom{x}}$  numerically and round)
- More remarkably, primality testing (Agrawal, Kayal, Saxena in 2002)

But trial division up to  $\sqrt{N}$  is not polynomial.

**Fundamental question:** Is there a polynomial time algorithm for factoring? This is unknown.

Later in this course we study the distribution of the prime numbers, in particular the function  $\pi(x)$ , the number of primes  $\leq x$ .

**Theorem 1.5.** There are infinitely many prime numbers, i.e.  $\lim_{x \rightarrow \infty} \pi(x) \rightarrow \infty$ .

*Proof.* Suppose there are only finitely many, say  $p_1, \dots, p_k$ . Consider  $N = \prod_{i=1}^k p_i + 1$ . Then  $N$  must be divisible by some prime other than the  $p_i$ , so we're done.  $\square$

All the largest known primes are of the form  $2^n - 1$  for  $n$  a prime. These are called **Mersenne primes**. 51 of them are known, the largest being  $2^{82589933} - 1$ .

## 2 Congruences

Fix a positive integer  $n$  (the modulus).

**Definition 2.1.** We say  $a \equiv b \pmod{n}$ , or that  $a$  is congruent to  $b \pmod{n}$  if  $n$  divides  $a - b$ .

This defines an equivalence relation on  $\mathbb{Z}$ , and we write  $\mathbb{Z}/n\mathbb{Z}$  for the set of equivalence classes. We can denote these by  $a + n\mathbb{Z}$ , or (more commonly) by  $a \pmod{n}$ . We can check that addition and multiplication are well-defined.

**Remark.**  $n\mathbb{Z}$  is a subgroup/ideal of  $\mathbb{Z}$  and  $\mathbb{Z}/n\mathbb{Z}$  is the quotient group/ring.

**Lemma 2.1.** Let  $a \in \mathbb{Z}/n\mathbb{Z}$ . Then the following are equivalent:

- (i)  $(a, n) = 1$
- (ii)  $\exists b \in \mathbb{Z}$  such that  $ab \equiv 1 \pmod{n}$
- (iii)  $a$  is a generator for  $\mathbb{Z}/n\mathbb{Z}$ .

*Proof.* (i)  $\implies$  (ii):  $(a, n) = 1 \implies \exists r, s \in \mathbb{Z}$  such that  $ra + sn = 1$ , so  $ra \equiv 1 \pmod{n}$ .

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

(ii)  $\iff$  (iii):  $\exists b \in \mathbb{Z}$  s.t.  $ab \equiv 1 \pmod{n} \iff 1$  belongs to the subgroup of  $\mathbb{Z}/n\mathbb{Z}$  generated by  $a$ .  $\square$

**Notation.**  $(\mathbb{Z}/n\mathbb{Z})^\times$  is the group of **units** in  $\mathbb{Z}/n\mathbb{Z}$ , i.e. the elements with an inverse under multiplication.

**Definition 2.2.**  $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$  is called the **Euler totient function**. We also have  $\phi(n) = |\{1 \leq a \leq n \mid (a, n) = 1\}|$ .

**Remark.**  $\mathbb{Z}/n\mathbb{Z}$  is a field  $\iff \phi(n) = n - 1 \iff n$  is prime.

**Theorem 2.2** (Euler-Fermat theorem). If  $(a, n) = 1$ , then  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

*Proof.* Apply Lagrange's theorem to the group  $G = (\mathbb{Z}/n\mathbb{Z})^\times$ . Then for  $a \in G$ , its order divides  $|G| = \phi(n)$ .  $\square$

As a corollary:

**Theorem 2.3** (Fermat's little theorem). If  $p \nmid a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .

**Lemma 2.4.** Let  $G$  be a cyclic group of order  $n$ . We have

$$|\{g \in G \mid \text{order}(g) = d\}| = \begin{cases} \phi(d) & \text{if } d \mid n \\ 0 & \text{otherwise} \end{cases}$$

In particular,  $\sum_{d \mid n} \phi(d) = n$ .

*Proof.* WLOG let  $G = (\mathbb{Z}/n\mathbb{Z}, +)$ . We have  $|\{g \in G \mid \text{order}(g) = n\}| \stackrel{(*)}{=} \phi(n)$  by Lemma 2.2. If  $d \mid n$ , say  $n = dk$ , then the elements of order dividing  $d$  are the classes  $0, k, 2k, \dots, (d-1)k \pmod{n}$ . These form a cyclic subgroup of order  $d$ . Applying  $(*)$  to this cyclic subgroup shows that there are  $\phi(d)$  elements of order  $d$ .  $\square$

**Example 2.1.** Consider the simultaneous linear congruences  $x \equiv 7 \pmod{10}$  and  $x \equiv 3 \pmod{13}$ . Suppose we can find  $u, v \in \mathbb{Z}$  such that

$$\begin{cases} u \equiv 1 \pmod{10} \\ u \equiv 0 \pmod{13} \end{cases}, \begin{cases} v \equiv 0 \pmod{10} \\ v \equiv 1 \pmod{13} \end{cases}.$$

Then  $x = 7u + 3v$  is a solution. But  $(10, 13) = 1 \implies \exists r, s \in \mathbb{Z}$  such that  $10r + 13s = 1$ , and we can just take  $u = 13s, v = 10r$ . To find  $r, s$ , we can use Euclid's algorithm to get  $r = 4, s = -3$ , so  $u = -39, v = 40$ , and so  $x \equiv 7 \cdot (-39) + 3 \cdot 40 \equiv 107 \pmod{130}$ .

**Theorem 2.5** (Chinese Remainder Theorem). Let  $m_1, \dots, m_k$  be pairwise coprime integers greater than 1. Let  $a_1, \dots, a_k \in \mathbb{Z}$ . Let  $M = m_1 m_2 \dots m_k$ . Then  $\exists x \in \mathbb{Z}$  satisfying

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

Moreover, the solution is unique mod  $M$ .

*Proof.* Uniqueness: Suppose  $x \equiv x' \pmod{m_i} \forall i$ . Then by considering the prime factorization of  $x - x'$  and using the fact that the  $m_i$  are pairwise coprime, we get  $x \equiv x' \pmod{M}$ .

Existence: Put  $M_i = \frac{M}{m_i}$ , so  $(M_i, m_i) = 1 \forall i$ . Hence we can find  $u_i \in \mathbb{Z}$  such that  $u_i M_i \equiv 1 \pmod{m_i} \forall i$ . Let  $x = \sum_{j=1}^k a_j u_j M_j$ . Then  $x \equiv a_i u_i M_i \equiv a_i \pmod{m_i}$ .  $\square$

We can write this theorem in one line using ring theory.

**Definition 2.3.** Let  $R_i = \mathbb{Z}/m_i\mathbb{Z}$ , and define  $R_1 \times \dots \times R_k = \{(r_1, \dots, r_k) \mid r_i \in R_i\}$  with addition and multiplication defined componentwise. This is a ring.

**Theorem 2.6** (CRT, ring-theoretic version). Let  $m_1, \dots, m_k$  be pairwise coprime integers greater than 1 and put  $M = m_1 \dots m_k$ . Then the map

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

is an isomorphism of rings.

*Proof.*  $\theta$  is a well defined ring homomorphism since  $m_i \mid M \forall i$ . Injectivity of  $\theta$  follows from uniqueness in CRT, and surjectivity of  $\theta$  follows from existence in CRT.  $\square$

**Corollary 2.7.**  $\theta$  induces an isomorphism of groups under multiplication

$$\begin{aligned} (\mathbb{Z}/M\mathbb{Z})^\times &\cong (\mathbb{Z}/m_1\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/m_k\mathbb{Z})^\times \\ a + M\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, \dots, a + m_k\mathbb{Z}). \end{aligned}$$

**Remark.** If  $a \in \mathbb{Z}$ , then  $(a, M) = 1 \iff (a, m_i) = 1 \forall i$ .

In particular, by looking at orders of the LHS and the RHS above, we get  $\phi(M) = \phi(m_1) \dots \phi(m_k)$ , i.e. the Euler phi function is multiplicative.

**Definition 2.4.** A function  $f : \mathbb{Z}^+ \rightarrow \mathbb{C}$  is **multiplicative** if  $f(mn) = f(m)f(n)$  whenever  $(m, n) = 1$ .

**Examples:**

- $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ ;
- $\tau(n) = \sum_{d|n} 1$ , the number of divisors of  $n$ ;
- $\sigma(n) = \sum_{d|n} d$ , the sum of divisors of  $n$ ;
- more generally,  $\sigma_k(n) = \sum_{d|n} d^k$ , so  $\sigma_0 = \tau$  and  $\sigma_1 = \sigma$ .

To prove this:

**Lemma 2.8.** If  $f : \mathbb{Z}^+ \rightarrow \mathbb{C}$  is multiplicative, then so is  $g : \mathbb{Z}^+ \rightarrow \mathbb{C}$ , defined by  $g(n) = \sum_{d|n} f(d)$ .

*Proof.* Let  $m, n$  be coprime. Note that every divisor  $d$  of  $mn$  can be written as  $d = d_1 d_2$ , where  $d_1 | m$ ,  $d_2 | n$  and  $(d_1, d_2) = 1$ . Thus

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

□

**Lemma 2.9.** (i) For  $p$  a prime,  $\phi(p^k) = p^{k-1}(p-1) = p^k(1 - \frac{1}{p})$ .

(ii)  $\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$ .

*Proof.* (i):  $\phi(p^k)$  counts the number of integers  $a$  between 1 and  $p^k$  such that  $(p^k, a) = (p, a) = 1$ . So we have  $p^a$  numbers, and we don't count the multiples of  $p$ , so  $\phi(p^k) = p^k - p^{k-1}$ .

(ii): Follows from the fact that  $\phi$  is multiplicative.

□

**Alternative proof** that  $\sum_{d|n} \phi(d) = n$  (cf Lemma 2.6).

*Proof.* Obviously the RHS is multiplicative. Since  $\phi(n)$  is multiplicative, the LHS is multiplicative by Lemma 2.13, so it suffices to check for  $n$  a prime power, say  $n = p^k$ . To this end, compute

$$\sum_{d|p^k} \phi(d) = \phi(1) + \phi(p) + \dots + \phi(p^k) = 1 + (p-1) + (p^2-p) + \dots + (p^k - p^{k-1}) = p^k.$$

□



## 2.1 Polynomial congruences

Let  $R = \mathbb{Z}, \mathbb{Q}, \mathbb{Z}/n\mathbb{Z}$  (or more generally any commutative ring). Set  $R[X] = \{\text{polynomials with coefficients in } R\}$ , i.e.  $a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$  for  $a_i \in R$ .

By definition, two polynomials are equal if and only if they have the same coefficients. We can check that  $R[X]$  is a ring (with usual  $+$  and  $\times$ ).

**Warning.** The map  $R[X] \rightarrow \{\text{functions } R \rightarrow R\}$  by  $f \mapsto (\alpha \mapsto f(\alpha))$  is not always injective. For example, if  $R = \mathbb{Z}/p\mathbb{Z}$  for  $p$  a prime, and  $f(X) = X^p - X$ , then  $f(\alpha) = 0 \forall \alpha \in R$ , but  $f$  is not the zero function.

**Question.** Can we show that if  $f \in R[X]$  has degree  $n$ , then  $f$  has at most  $n$  roots in  $R$ ?

**Answer.** No. For example, take  $R = \mathbb{Z}/8\mathbb{Z}$ , then  $f(X) = X^2 - 1$  has 4 solutions in  $\mathbb{Z}/8\mathbb{Z}$ .

Let  $R = \mathbb{Z}, \mathbb{Q}, \mathbb{Z}/n\mathbb{Z}$  (or any commutative ring).

We have a **division algorithm** on  $R[X]$ :

Let  $f, g \in R[X]$  and suppose the leading coefficient of  $g$  is a unit. Then  $\exists q, r \in R[X]$  such that  $f(X) = Q(X)g(X) + r(X)$  and  $\deg(r) < \deg(g)$ .

*Proof.* By induction on  $\deg(f)$ . If  $\deg(f) < \deg(g)$ , take  $q = 0, r = f$ . Otherwise, let  $f(X) = aX^m + \dots$  and  $g(X) = bX^n + \dots$  with  $m \geq n$  and  $b$  a unit.

Let  $f_1(X) = f(X) - ab^{-1}X^{m-n}g(X)$ . Then  $\deg(f_1) < \deg(f)$ , so by the induction hypothesis,  $f_1(x) = q_1(x)g(x) + r_1(x)$  for some  $q_1, r_1 \in R[X]$  and  $\deg(r_1) < \deg(g)$ . Now take  $q(X) = ab^{-1}X^{m-n} + q_1(X)$  and  $r = r_1$ , so we're done.  $\square$

**Corollary 2.10.** If  $f \in R[X]$  and  $\alpha \in R$  is such that  $f(\alpha) = 0$ , then  $f(X) = (X - \alpha)f_1(X)$  for some  $f_1 \in R[X]$ .

*Proof.* By the division algorithm,  $f(X) = (X - \alpha)f_1(X) + r$  for some  $r \in R$  (as  $\deg(r) < \deg(X - \alpha)$ ). Plug in  $X = \alpha$  to get  $r = 0$ .  $\square$

**Definition 2.5.**  $R$  is an **integral domain** if  $R$  has no zero divisors, i.e.  $\alpha, \beta \in R, \alpha\beta = 0 \implies \alpha = 0$  or  $\beta = 0$ .

**Note.** Let  $n > 1$ . Then  $\mathbb{Z}/n\mathbb{Z}$  is an integral domain  $\iff n$  is prime.

**Theorem 2.11.** If  $R$  is an integral domain, then any polynomial  $f \in R[X]$  of degree  $n$  has at most  $n$  roots.

*Proof.* By induction on  $n$ , the degree of  $f$ . If  $n = 0$ , then our polynomial is a nonzero constant and we're done. Now suppose  $\exists \alpha \in R$  such that  $f(\alpha) = 0$  (otherwise we're done). By Corollary 2.10,  $f(X) = (X - \alpha)f_1(X)$ . Since  $R$  is an integral domain, every root of  $f$ , except possibly  $\alpha$  is a root of  $f_1$ . By induction,  $f_1$  has at most  $n - 1$  roots, hence  $f$  has at most  $n$  roots and we're done.  $\square$

13 Oct 2022,  
Lecture 4

**Corollary 2.12** (Lagrange's Theorem). Let  $p$  be a prime and  $a_0, \dots, a_n \in \mathbb{Z}$  with  $p \nmid a_n$ . Then the congruence

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod{p}$$

has at most  $n$  solutions mod  $p$ .

*Proof.* Take  $R = \mathbb{Z}/p\mathbb{Z}$  in Theorem 2.17. □

**Remark.** In this course, we will refer to the above theorem as Lagrange's Theorem.

**Example 2.2.** Let  $p$  be a prime. We will factor  $X^{p-1} - 1 \pmod{p}$ . Let  $f(X) = X^{p-1} - 1 - \prod_{a=1}^{p-1} (X - a)$  in  $\mathbb{Z}/p\mathbb{Z}[X]$ . By Fermat's Little Theorem,  $f$  has at least  $p-1$  roots mod  $p$ . But  $\deg(f) < p-1$ , since the  $X^{p-1}$  terms cancel out, so by Lagrange's Theorem,  $f = 0$ , i.e.  $X^{p-1} - 1 = \prod_{a=1}^{p-1} (X - a)$  in  $\mathbb{Z}/p\mathbb{Z}[X]$ . Plugging in  $X = 0$  gives  $(p-1)! \equiv -1 \pmod{p}$ , i.e. Wilson's Theorem.

**Example 2.3.** Working mod 7, the powers of 3 (starting from 0) are 1, 3, 2, 6, 4, 5. So  $(\mathbb{Z}/7\mathbb{Z})^\times$  is cyclic, generated by 3.

**Theorem 2.13.** Let  $p$  be a prime. Then  $(\mathbb{Z}/p\mathbb{Z})^\times$  is cyclic.

*Proof.* Let  $S_d = \{a \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \text{ord}(a) = d\}$ . Suppose  $S_d \neq \emptyset$ , say  $a \in S_d$ . Then  $1, a, a^2, \dots, a^{d-1}$  are distinct elements in  $\mathbb{Z}/p\mathbb{Z}$  and they are solutions of  $x^d \equiv 1 \pmod{p}$ . By Lagrange's theorem, this has at most  $d$  solutions, and we found  $d$  solutions, so those are all of them, i.e.  $S_d \subseteq \{1, a, a^2, \dots, a^{d-1}\}$ . Note that the LHS is a cyclic group of order  $d$ , so this has  $\phi(d)$  elements of order  $d$ .

We conclude that for every  $d$ ,  $|S_d| = 0$  or  $|S_d| = \phi(d)$ . In particular,  $|S_d| \leq \phi(d)$ . Hence

$$p-1 \stackrel{(\star)}{=} \sum_{d \mid (p-1)} |S_d| \leq \sum_{d \mid (p-1)} \phi(d) = p-1,$$

where  $(\star)$  follows since we just count all the elements in  $(\mathbb{Z}/p\mathbb{Z})^\times$ . Hence  $|S_d| = \phi(d) \forall d \mid (p-1)$ . In particular,  $S_{p-1} \neq \emptyset$ , i.e.  $(\mathbb{Z}/p\mathbb{Z})^\times$  contains elements of order  $p-1$ , i.e.  $(\mathbb{Z}/p\mathbb{Z})^\times$  is cyclic. □

**Remark.** The same argument shows that any finite subgroup of the multiplicative group of a field is cyclic.

**Definition 2.6.** An integer  $a$  such that  $a \pmod{n}$  generates  $(\mathbb{Z}/n\mathbb{Z})^\times$  is called a **primitive root** mod  $n$ .

Theorem 2.21 showed that primitive roots exist mod  $p$ .

**Example 2.4.** Let  $p = 19$ . Let  $d$  be the order of 2 in  $(\mathbb{Z}/19\mathbb{Z})^\times$ . We know  $d \mid 18$ , so we work out

$$\begin{aligned} 2^3 &\equiv 8 \pmod{19} \\ 2^6 &\equiv 7 \not\equiv 1 \pmod{19} \implies d \nmid 6 \\ 2^9 &\equiv -1 \not\equiv 1 \pmod{19} \implies d \nmid 9, \end{aligned}$$

so  $d = 18$  and hence 2 is a primitive root mod 19.

In general,  $g \in \mathbb{Z}$  (coprime to  $p$ ) is a primitive root mod  $p$  if and only if  $g^{\frac{p-1}{q}} \not\equiv 1 \pmod{p} \quad \forall \text{ primes } q \mid (p-1)$ .

**Remark.** The number of primitive roots mod  $p$  is  $\phi(p-1) = \phi(\phi(p))$ .

Here are some (open) problems concerning primitive roots:

- (i) Artin's conjecture (1927) – Let  $a > 1$  be an integer which is not a square. Then  $a$  is a primitive root mod  $p$  for infinitely many primes  $p$ . This is unknown for  $a = 2$ . Hooley (1967) proved this assuming GRH. Heath-Brown (1986) proved that Artin's conjecture holds for at least one of 2, 3 or 5. In fact, he proved something stronger: he proved the conjecture fails for at most 2 prime values of  $a$ .
- (ii) How large is the smallest primitive root mod  $p$ ? Burgess (1962) showed it is  $\leq cp^{1/4+\epsilon} \quad \forall \epsilon > 0$  and some constant  $c = c(\epsilon)$ . Shoup (1992) showed it is  $\leq c(\log p)^6$  assuming GRH.

We now consider  $\mathbb{Z}/p^n\mathbb{Z}$  for  $n > 1$ . For  $n \geq 3$ , there is a surjective group homomorphism from  $(\mathbb{Z}/2^n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/8\mathbb{Z})^\times = \{\pm 1, \pm 3\} \cong C_2 \times C_2$ , so  $(\mathbb{Z}/2^n\mathbb{Z})^\times$  is not cyclic (since generators map to generators).

**Theorem 2.14.** Let  $p$  be an odd prime. Then  $(\mathbb{Z}/p^n\mathbb{Z})^\times$  is cyclic  $\forall n \geq 1$ .

We divide the proof into 3 lemmas.

**Lemma 2.15.** Let  $n \geq 2$ . Then  $g$  is a primitive root mod  $p^n$  if and only if the following two conditions hold:

$$\begin{cases} g \text{ is a primitive root mod } p \\ g^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n} \end{cases}.$$

*Proof.* ( $\implies$ ) is clear, as  $\phi(p^n) = p^{n-1}(p-1)$ .

( $\impliedby$ ): Let  $d$  be the order of  $g$  in  $(\mathbb{Z}/p^n\mathbb{Z})^\times$ . Then  $d \mid \phi(p^n) = p^{n-1}(p-1)$ . Since  $g^d \equiv 1 \pmod{p^n}$ , we have  $g^d \equiv 1 \pmod{p}$ . Hence by assumption 1, we have  $(p-1) \mid d$ . Say  $d = p^j(p-1)$  for some  $0 \leq j \leq n-1$ . If  $j \leq n-2$ , then this contradicts assumption 2. Hence  $j = n-1$ , so  $d = \phi(p^n)$  is a primitive root mod  $p^n$ .  $\square$

Next we show  $\exists g \in \mathbb{Z}$  satisfying conditions 1 and 2 in the case  $n = 2$ .

**Lemma 2.16.**  $\exists g \in \mathbb{Z}$  a primitive root mod  $p$  such that  $g^{p-1} \not\equiv 1 \pmod{p^2}$ .

*Proof.* Let  $g$  be a primitive root mod  $p$ . If  $g^{p-1} \equiv 1 \pmod{p^2}$ , then consider  $g + p$ , which is still a primitive root mod  $p$ , but

$$(g + p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + \dots \equiv 1 + (p-1)g^{p-2}p \pmod{p^2},$$

where the second term is not divisible by  $p^2$ , so  $(g + p)^{p-1} \not\equiv 1 \pmod{p^2}$ .  $\square$

Next we show that if  $g$  is a primitive root mod  $p^2$ , then it is a primitive root mod  $p^n \forall n \geq 2$ .

**Lemma 2.17.** If  $g^{p-1} \not\equiv 1 \pmod{p^2}$ , then  $g^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n} \forall n \geq 2$ .

*Proof.* By induction on  $n$ , the case  $n = 2$  being given. Suppose the result is true for  $n$ . By Euler-Fermat,  $g^{p^{n-2}(p-1)} \equiv 1 \pmod{p^{n-1}}$ , so  $g^{p^{n-2}(p-1)} = 1 + bp^{n-1}$  for some  $b \in \mathbb{Z}$ , where  $p \nmid b$  by the induction hypothesis. Taking  $p^{\text{th}}$  powers gives

$$\begin{aligned} g^{p^{n-1}(p-1)} &= (1 + bp^{n-1})^p = 1 + bp^n + \binom{p}{2}b^2p^{2(n-1)} + \dots \equiv \\ &1 + bp^n + \binom{p}{2}b^2p^{2(n-1)} \stackrel{\star}{\equiv} 1 + bp^n \pmod{p^{n+1}}, \end{aligned}$$

where  $\star$  follows since  $p$  is odd, so  $p \mid \binom{p}{2}$  (and also we use  $3(n-1) \geq n+1$  and  $2(n-1)+1 \geq n+1$ ). Thus  $g^{p^{n-1}(p-1)} \equiv 1 + bp^n \not\equiv 1 \pmod{p^{n+1}}$ , so the result follows for  $n+1$ .  $\square$

This completes the proof of Theorem 2.24.

**Example 2.5.** We saw 3 is a primitive root mod 7. We calculate  $3^3 = -1 + 4 \cdot 7$ , so  $3^6 \equiv 1 - 8 \cdot 7 \not\equiv 1 \pmod{7^2}$ . Hence 3 is a primitive root mod  $7^n \forall n$ .

For the case  $p = 2$ , let  $G = \{a \in (\mathbb{Z}/2^n\mathbb{Z})^\times \mid a \equiv 1 \pmod{4}\}$ . Then  $(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \{\pm 1\} \times G$  by  $a + 2^n\mathbb{Z} \mapsto \begin{cases} (1, a + 2^n\mathbb{Z}) & \text{if } a \equiv 1 \pmod{4} \\ (-1, -a + 2^n\mathbb{Z}) & \text{if } a \equiv 3 \pmod{4} \end{cases}$ .

**Exercise.** Show that  $G$  is cyclic (and generated by 5).

**Exercise.** For which  $n$  is  $(\mathbb{Z}/n\mathbb{Z})^\times$  cyclic?

18 Oct 2022,  
Lecture 6

### 3 Quadratic residues

Let  $p$  be an odd prime and  $a \in \mathbb{Z}$ . By Lagrange's theorem, the congruence  $x^2 \equiv a \pmod{p}$  has at most 2 solutions. If  $a \not\equiv 0 \pmod{p}$ , then there are either 0 or 2 solutions. Indeed, if  $x$  is a solution, then so is  $-x \not\equiv x \pmod{p}$ .

**Definition 3.1.** Suppose  $a \not\equiv 0 \pmod{p}$ . We say  $a$  is a **quadratic residue** (QR) if  $x^2 \equiv a \pmod{p}$  is soluble. We say  $a$  is a **quadratic nonresidue** (QNR) if  $x^2 \equiv a \pmod{p}$  is unsoluble.

**Example 3.1.**  $p = 7$ . 1, 2, 4 are QRs and 3, 5, 6 are QNRs.

**Lemma 3.1.** Let  $p$  be an odd prime. Then there are  $\frac{p-1}{2}$  quadratic residues mod  $p$  (and hence also  $\frac{p-1}{2}$  quadratic nonresidues).

*Proof 1.* Let  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  (a field with  $p$  elements). We show that the map  $\mathbb{F}_p^\times \rightarrow \mathbb{F}_p^\times$  by  $x \mapsto x^2$  is exactly 2-to-1.

Indeed, if  $x^2 \equiv y^2 \pmod{p}$ , then  $p \mid x^2 - y^2$ , so  $p \mid (x - y)$  or  $p \mid (x + y)$ , so  $x \equiv \pm y \pmod{p}$ .  $\square$

*Proof 2.* Let  $g$  be a primitive root mod  $p$ . Then  $\mathbb{F}_p^\times = \{1, g, g^2, \dots, g^{p-2}\}$ .

We claim that  $g^i$  is a QR  $\iff i$  is even.

$\Leftarrow$  is clear. For  $\Rightarrow$ , suppose  $g^i \equiv x^2 \pmod{p}$ . Then we can write  $x = g^j \pmod{p}$ , so  $g^i \equiv g^{2j} \pmod{p} \implies i \equiv 2j \pmod{p-1}$ . But  $p-1$  is even, so  $i = 2j + k(p-1)$  is even.  $\square$

**Definition 3.2** (Legendre symbol). Let  $p$  be an odd prime,  $a \in \mathbb{Z}$ . Then

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

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

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

*Proof.* This is obvious if  $p \mid a$ , so suppose  $(a, p) = 1$ . By Fermat's little theorem,  $a^{p-1} \equiv 1 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ .

If  $\left(\frac{a}{p}\right) = 1$ , then  $a \equiv b^2 \pmod{p}$  for some  $b \in \mathbb{Z}$ , but then  $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$ . This gives  $\frac{p-1}{2}$  solutions to the congruence  $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ . By Lagrange's theorem, these are all the solutions. Hence if  $\left(\frac{a}{p}\right) = -1$ , then  $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ , so  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$  and we're done.  $\square$

**Corollary 3.3.**  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$ .

*Proof.*

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

Since  $0, \pm 1$  are distinct mod  $p$ , we have equality in the above.  $\square$

The corollary is equivalent to the statements:

- $\mathcal{X} : \mathbb{F}_p^\times \rightarrow \{\pm 1\}$  by  $a \mapsto \left(\frac{a}{p}\right)$  is a group homomorphism.
- (i)  $\text{QR} \cdot \text{QR} = \text{QR}$   
(ii)  $\text{QR} \cdot \text{QNR} = \text{QNR}$   
(iii)  $\text{QNR} \cdot \text{QNR} = \text{QR}$

We can give an alternative proof for this:

- (i)  $a \equiv x^2 \pmod{p}, b \equiv y^2 \pmod{p} \implies ab \equiv (xy)^2 \pmod{p}$ .
- (ii) If  $a \equiv x^2$  and  $ab \equiv z^2 \pmod{p}$ , then  $b \equiv (x^{-1}z)^2 \pmod{p}$ , a contradiction.
- (iii) Suppose  $a$  is a QNR. The map  $\mathbb{F}_p^\times \rightarrow \mathbb{F}_p^\times$  by  $x \mapsto ax$  is a bijection sending QRs to NQRs by (ii). By Lemma 3.1, it sends QNRs to QRs, done.

**Remark.** We can also prove Euler's criterion using primitive roots.

**Corollary 3.4.** Let  $p$  be an odd prime. Then

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

In the next lecture, we show

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

Let  $p, q$  be distinct odd primes. The law of quadratic reciprocity gives a relation between  $\left(\frac{p}{q}\right)$  and  $\left(\frac{q}{p}\right)$ . Generalizing this result (in many different ways) has been one of the main goals of number theory ever since.

**Theorem 3.5** (Law of quadratic reciprocity). Let  $p, q$  be distinct odd primes. Then

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

**Example 3.2.**

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

**Another proof of Fermat's little theorem:**

If  $(a, p) = 1$ , then working mod  $p$ , the set  $\{a, 2a, 3a, \dots, (p-1)a\}$  is the same as  $\{1, 2, \dots, (p-1)\}$ . Taking the product gives  $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p} \implies a^{p-1} \equiv 1 \pmod{p}$  as desired.

We can use the same idea to compute  $a^{\frac{p-1}{2}} \pmod{p}$ :

20 Oct 2022,  
Lecture 7

**Lemma 3.6** (Gauss' Lemma). Let  $p$  be an odd prime, let  $a \in \mathbb{Z}$  be coprime to  $p$ , and put  $m = \frac{p-1}{2}$ . For  $j = 1, 2, \dots, m$  let  $a_j$  be the unique integer such that

$$(i) \quad a_j \equiv ja \pmod{p}$$

$$(ii) \quad -m \leq a_j \leq m.$$

Then  $\left(\frac{a}{p}\right) = (-1)^\nu$ , where  $\nu = \#\{1 \leq j \leq m \mid a_j < 0\}$ .

*Proof.* Consider  $a_1, \dots, a_m \in \{\pm 1, \pm 2, \dots, \pm m\}$ . Can any two of these be the same? No, since  $a_i \equiv a_j \implies ai \equiv aj \implies i \equiv j \pmod{p}$ .

Can any two differ by a sign? No, since  $a_i \equiv -a_j \implies ia \equiv -ja \implies i \equiv -j \pmod{p}$ .

Hence  $a_1, \dots, a_m$  are  $\pm 1, \pm 2, \dots, \pm m$  in some order with some choice of signs. Taking the product gives

$$a_1 \dots a_m \equiv (-1)^\nu 1 \cdot \dots \cdot m \pmod{p} \implies a^m m! \equiv (-1)^\nu m! \pmod{p}.$$

So by Euler's criterion,  $\left(\frac{a}{p}\right) \equiv a^m \equiv (-1)^\nu \pmod{p}$ . □

**Corollary 3.7.** Let  $p$  be an odd prime. Then

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

*Proof.* Let  $m = \frac{p-1}{2}$ . Then  $a_j = \begin{cases} 2j & \text{for } 1 \leq j \leq \frac{m}{2}. \\ 2j - p & \text{for } \frac{m}{2} < j \leq m. \end{cases}$  Hence

$$\nu = m - \left\lfloor \frac{m}{2} \right\rfloor = \begin{cases} \frac{m}{2} & \text{if } m \text{ is even.} \\ \frac{m+1}{2} & \text{if } m \text{ is odd.} \end{cases}$$

It follows that  $\left(\frac{2}{p}\right) = 1 \iff \nu \text{ is even} \iff m \equiv 0, 3 \pmod{4} \iff p \equiv \pm 1 \pmod{8}$ . □

**Theorem 3.8** (Law of quadratic reciprocity). Let  $p, q$  be distinct odd primes. Then

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

*Proof.* Step 1: Let  $a, p, \nu$  be as in Gauss' Lemma (with  $a \geq 1$ ).

Claim:

$$\nu = \sum_{i=1}^{2n} (-1)^i \left\lfloor \frac{ip}{2a} \right\rfloor$$

where  $n = \lfloor \frac{a}{2} \rfloor$ . Moreover,  $\frac{ip}{2a} \notin \mathbb{Z} \forall 1 \leq i \leq 2n$ .

Proof: Consider all multiples of  $a$  less than  $\frac{ap}{2}$  ( $= np$  or  $(n + \frac{1}{2})p$ ). Hence  $\nu$  is the number of multiples of  $a$  in the intervals

$$\left[ \frac{1}{2}p, p \right], \left[ \frac{3}{2}p, 2p \right], \dots, \left[ (n - \frac{1}{2})p, np \right].$$

On dividing through by  $a$ , we see that  $\nu$  is the number of integers in

$$\left[ \frac{p}{2a}, \frac{2p}{2a} \right], \left[ \frac{3p}{2a}, \frac{4p}{2a} \right], \dots, \left[ \frac{(2n-1)p}{2a}, \frac{2np}{2a} \right].$$

The end points are not in  $\mathbb{Z}$ , since the end points of the original intervals are not multiples of  $a$ . Hence  $\#([\alpha, \beta] \cap \mathbb{Z}) = \lfloor \beta \rfloor - \lfloor \alpha \rfloor$ . This proves the claim.

Step 2: Let  $p_1, p_2$  be primes and  $a \in \mathbb{Z}$  coprime to  $p_1 p_2$ . By Gauss' lemma,  $\left( \frac{a}{p_i} \right) = (-1)^{\nu_i}$ .

- (i) Suppose  $p_1 \equiv p_2 \pmod{4a}$ . Then  $\lfloor \frac{ip_1}{2a} \rfloor \equiv \lfloor \frac{ip_2}{2a} \rfloor \pmod{2}$ . By Step 1, we have  $\nu_1 \equiv \nu_2 \pmod{2}$ . Hence  $\left( \frac{a}{p_1} \right) = \left( \frac{a}{p_2} \right)$ .
- (ii) Suppose  $p_1 \equiv -p_2 \pmod{4a}$ . Then  $\lfloor \frac{ip_1}{2a} \rfloor \equiv \lfloor \frac{ip_2}{2a} \rfloor + 1 \pmod{2}$ . (We use the fact that if  $\alpha \in \mathbb{R}/\mathbb{Z}$ , then  $\lfloor -\alpha \rfloor = -\lfloor \alpha \rfloor - 1$ ). By Step 1, we again deduce  $\left( \frac{a}{p_1} \right) = \left( \frac{a}{p_2} \right)$ .

Step 3: Conclusion of the proof.

- (i) Suppose  $p \equiv q \pmod{4}$ , say  $p = 4a + q$ . Then  $\left( \frac{p}{q} \right) = \left( \frac{4a+q}{q} \right) = \left( \frac{a}{q} \right)$ , and  $\left( \frac{q}{p} \right) = \left( \frac{p-4a}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{a}{p} \right)$ . But  $p \equiv q \pmod{4a} \xrightarrow{\text{Step 2(i)}} \left( \frac{a}{p} \right) = \left( \frac{a}{q} \right)$ , hence we conclude

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

- (ii) Suppose  $p \not\equiv q \pmod{4}$ , say  $p + q = 4a$ . Then  $\left( \frac{p}{q} \right) = \left( \frac{4a-q}{q} \right) = \left( \frac{a}{q} \right)$  and  $\left( \frac{q}{p} \right) = \left( \frac{4a-p}{p} \right) = \left( \frac{a}{p} \right)$ . But  $p \equiv -q \pmod{4a} \xrightarrow{\text{Step 2(ii)}} \left( \frac{a}{p} \right) = \left( \frac{a}{q} \right)$ , so  $\left( \frac{p}{q} \right) = \left( \frac{q}{p} \right)$ , done.

□

22 Oct 2022,  
Lecture 8

**Example 3.3.** Compute the Legendre symbol  $\left( \frac{7411}{9283} \right)$ . In fact, 7411 and 9283 are both prime. Hence

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



As  $1872 = 2^4 \cdot 3^2 \cdot 13$ , we get

$$-\left(\frac{1872}{8411}\right) = -\left(\frac{13}{7411}\right) = -\left(\frac{7411}{13}\right) = -\left(\frac{1}{13}\right) = -1.$$

Hence 7411 is not a QR mod 9283.

Recall that the Legendre symbol  $\left(\frac{a}{p}\right)$  is only defined for  $p$  an odd prime.

**Definition 3.3.** Let  $n$  be an odd positive integer, say  $n = p_1 \dots p_k$  for  $p_i$  (not necessarily distinct) odd primes. Let  $a \in \mathbb{Z}$ . We define the **Jacobi symbol** as

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

**Remark.** If  $(a, n) \neq 1$ , then  $\left(\frac{a}{n}\right) = 0$ .

**Proposition 3.9.** (i)  $\left(\frac{a}{n}\right)$  depends only on  $a \bmod n$ .

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

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

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

*Proof.* (i) Clear, since the Legendre symbol only depends on  $a \bmod p$ .

(ii) The first part follows since the Legendre symbol is totally multiplicative, and the second follows from the definition of the Jacobi symbol.

(iii) This holds for  $n = p$  a prime by previous results. We will now show that if they hold for odd integers  $m, n$ , then they hold for  $mn$ . But

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

where we can check that  $\star$  holds, since  $(m-1)(n-1) \equiv 0 \pmod{4}$ , which gives  $mn-1 \equiv (m-1) + (n-1) \pmod{4}$ .

(iv) This is analogous to above, except we get

$$(-1)^{\frac{m^2-1}{8}} (-1)^{\frac{n^2-1}{8}} = (-1)^{\frac{(mn)^2-1}{8}},$$

since  $(m^2-1)(n^2-1) \equiv 0 \pmod{16}$ , so  $(mn)^2-1 \equiv (m^2-1) + (n^2-1) \pmod{16}$ .

□

**Theorem 3.10** (Law of Quadratic Reciprocity for Jacobi Symbols). If  $m, n$  are odd positive integers, then

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

**Remark.** If  $(m, n) \neq 1$ , this says  $0 = 0$ .

*Proof.* Again, we deduce this from the corresponding result for the Legendre symbol. Assume  $(m, n) = 1$ . Write  $m = \prod_{i=1}^k p_i$  and  $n = \prod_{j=1}^l q_j$  for  $p_i, q_j$  (not necessarily distinct) primes.

Let  $r$  count the number of  $p_i$  with  $p_i \equiv 3 \pmod{4}$  and  $s$  count the number of  $q_j$  with  $q_j \equiv 3 \pmod{4}$ . Then

$$\begin{aligned} \left(\frac{m}{n}\right) &= \prod_{i=1}^k \prod_{j=1}^l \left(\frac{p_i}{q_j}\right) = \prod_{i=1}^k \prod_{j=1}^l (-1)^{\frac{p_i-1}{2} \frac{q_j-1}{2}} \left(\frac{q_j}{p_i}\right) = \\ &= (-1)^{rs} \prod_{i=1}^k \prod_{j=1}^l \left(\frac{q_j}{p_i}\right) = (-1)^{rs} \left(\frac{n}{m}\right). \end{aligned}$$

But  $m \equiv 1 \pmod{4} \iff r$  is even, and  $n \equiv 1 \pmod{4} \iff s$  is even, hence  $(-1)^{rs} = (-1)^{\frac{m-1}{2} \frac{n-1}{2}}$ .  $\square$

**Remark.** The Jacobi symbol  $\left(\frac{a}{n}\right)$  tells us surprisingly little about whether the congruence  $x^2 \equiv a \pmod{n}$  is soluble.

If  $x^2 \equiv a \pmod{n}$  is soluble, then so is  $x^2 \equiv a \pmod{p}$  for all primes  $p \mid n$ . So  $\left(\frac{a}{p}\right) = 1 \forall p \mid n$ , hence  $\left(\frac{a}{n}\right) = 1$ .

But the converse is false. For example,  $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1$ , yet  $x^2 \equiv 2 \pmod{15}$  is not soluble.

The point of the Jacobi symbol is rather that it allows us to compute Legendre symbols without having to factor (except for removing powers of 2).

**Example 3.4.**

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

so 33 is not a QR mod 73.

Three tricks to evaluate Legendre symbols:

**Example 3.5.** (i)  $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$

(ii)  $\sum_{a=1}^{p-1} a \left(\frac{a}{p}\right) \equiv 0 \pmod{p}$  if  $p > 3$ .

$$(iii) \sum_{a=1}^{p-1} \left( \frac{a(a+1)}{p} \right) \equiv -1.$$

*Proof.* (i) We have already done this since we have an equal number of QRs and QNRs. However, alternate proof:

Let  $b$  be a QNR  $(\text{mod } p)$ . Then

$$\sum_{a=1}^{p-1} \left( \frac{a}{p} \right) = \sum_{a=1}^{p-1} \left( \frac{ab}{p} \right) = \left( \frac{b}{p} \right) \sum_{a=1}^{p-1} \left( \frac{a}{p} \right) = - \sum_{a=1}^{p-1} \left( \frac{a}{p} \right),$$

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

(ii) Since  $p > 3$ , we can choose  $b \not\equiv 0, \pm 1 \pmod{p}$ , whence

$$\sum_{a=1}^{p-1} a \left( \frac{a}{p} \right) \equiv \sum_{a=1}^{p-1} ab \left( \frac{ab}{p} \right) \equiv \pm b \sum_{a=1}^{p-1} a \left( \frac{a}{p} \right) \pmod{p}.$$

Since  $b \not\equiv \pm 1 \pmod{p}$ , we deduce  $\sum_{a=1}^{p-1} a \left( \frac{a}{p} \right) \equiv 0 \pmod{p}$ .

(iii) If  $ab \equiv 1 \pmod{p}$ , then

$$\left( \frac{a(a+1)}{p} \right) \equiv \left( \frac{a^2(1+b)}{p} \right) = \left( \frac{b+1}{p} \right).$$

Then

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

□

## 4 Binary quadratic forms

**Question.** Which numbers can be written as the sum of two squares?

Fermat gave an answer around 1630, and Euler published the first proof in 1749.

**Theorem 4.1.** Let  $N$  be a positive integer. Then  $N$  is the sum of two squares if and only if every prime  $p \equiv 3 \pmod{4}$  that divides  $N$  divides it to an even power.

*Proof of the easy direction.*  $\implies$  : Suppose  $N = x^2 + y^2$  and  $p \mid N$ , then  $x^2 + y^2 \equiv 0 \pmod{p}$ . If  $p \equiv 3 \pmod{4}$ , then  $\left( \frac{-1}{p} \right) = -1$ , so we must have  $x \equiv y \equiv 0 \pmod{p}$ . Then divide  $N$  by  $p^2$  and repeat until  $p \nmid N$ .

25 Oct 2022,  
Lecture 9

$\Leftarrow$  : Since  $(x^2 + y^2)(z^2 + t^2) = (xz - yt)^2 + (xt + yz)^2$ , it suffices to prove the result the case  $N = p$  with  $p = 2$  or  $p \equiv 1 \pmod{4}$ .  $p = 2$  is easy, but  $p \equiv 1 \pmod{4}$  is a little more involved, and we will prove it a later lecture.  $\square$

Euler also studied  $x^2 + 2y^2, x^2 + 3y^2$ , etc. In this section we study **binary quadratic forms** with integer coefficients, i.e.  $f(x, y) = ax^2 + bxy + cy^2$  for  $a, b, c \in \mathbb{Z}$ .

**Definition 4.1.** We say  $f$  **represents**  $n$  if  $f(x, y) = n$  for some  $x, y \in \mathbb{Z}$ .

We may write  $f$  as  $(a, b, c)$  or in matrix notation as

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

**Example 4.1.**  $f(x, y) = x^2 + y^2$  may be written as  $(1, 0, 1)$  or  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ .

$g(x, y) = 4x^2 + 12xy + 10y^2$  may be written as  $(4, 12, 10)$  or  $\begin{pmatrix} 4 & 6 \\ 6 & 10 \end{pmatrix}$ .

Note that  $g(x, y) = (2x + 3y)^2 + y^2 = f(2x + 3y, y)$ . Do  $f$  and  $g$  represent the same numbers? No, as  $g$  only represents even numbers.

Let  $X = 2x + 3y, Y = y$ , then

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

Note that we can have  $X, Y \in \mathbb{Z}$ , yet  $x, y \notin \mathbb{Z}$ .

**Definition 4.2.** A **unimodular substitution** is one of the form  $X = \alpha x + \gamma y, Y = \beta x + \delta y$  where  $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$  and  $\alpha\delta - \beta\gamma = 1$ .

**Definition 4.3.** Two BQFs  $f$  and  $g$  are **equivalent**, written  $f \sim g$ , if they are related by a unimodular substitution.

Exercise: Check  $\sim$  is an equivalence relation (this is on the example sheet).

**Note.** Equivalent forms represent the same integers.

The group  $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mid \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \alpha\delta - \beta\gamma = 1 \right\}$  acts on the set of BQFs via  $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : f(x, y) \mapsto f(\alpha x + \gamma y, \beta x + \delta y)$ . The equivalence classes are the orbits of this action.

To check a group action, we need to check

- (i)  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} f = f$ , which is true.

(ii)  $\sigma(\tau f) = (\sigma\tau)f \ \forall \sigma, \tau \in SL_2(\mathbb{Z})$ .

Suppose  $f = (a, b, c)$  and  $g = (a', b', c')$  are equivalent, say  $g = \sigma f$  for  $\sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ . Then

$$g(x, y) = f(\alpha x + \gamma y, \beta x + \delta y) = (\alpha x + \gamma y \quad \beta x + \delta y) \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} \alpha x + \gamma y \\ \beta x + \delta y \end{pmatrix} = \\ (x \quad y) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Hence  $\begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix} = \sigma \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \sigma^\top$ . Call this  $(\star)$ .

To check (ii), we note that

$$\sigma \left( \tau \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \tau^\top \right) \sigma^\top = (\sigma\tau) \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} (\sigma\tau)^\top.$$

**Definition 4.4.** The **discriminant** of  $f(x, y) = ax^2 + bxy + cy^2$  is

$$\text{disc}(f) = b^2 - 4ac.$$

**Example 4.2.**  $\text{disc}(1, 0, 1) = -4$ ,  $\text{disc}(4, 12, 10) = -16$ .

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

*Proof.* Taking determinants in  $(\star)$  gives

$$a'c' - \left(\frac{b'}{2}\right)^2 = (\det \sigma)^2 \left( ac - \left(\frac{b}{2}\right)^2 \right).$$

But  $\det \sigma = 1$ , so multiplying both sides by  $-4$  gives  $(b')^2 - 4a'c' = b^2 - 4ac$  as desired.  $\square$

**Remark.** The converse is not true, i.e. there exist BQFs with the same discriminant which are not equivalent.

For example,  $(1, 0, 6)$  and  $(2, 0, 3)$  both have discriminant  $-24$ , but  $(1, 0, 6)$  represents 1 (with  $x = 1, y = 0$ ), but  $(2, 0, 3)$  does not.

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

*Proof.*  $\implies$  :  $d = b^2 - 4ac \equiv b^2 \equiv 0, 1 \pmod{4}$ .

$\impliedby$  : If  $d \equiv 0 \pmod{4}$ , let  $f = (1, 0, -\frac{d}{4})$ . If  $d \equiv 1 \pmod{4}$ , take  $f = (1, 1, \frac{1-d}{4})$ .  $\square$

**Definition 4.5.** A quadratic form  $f(x_1, \dots, x_n) = \sum_{i \leq j} a_{ij} x_i x_j$  with  $a_{ij} \in \mathbb{R}$  is:

- **positive definite** if  $f(x) > 0 \forall 0 \neq x \in \mathbb{R}^n$ .
- **negative definite** if  $f(x) < 0 \forall 0 \neq x \in \mathbb{R}^n$ .
- **indefinite** if  $f(x) > 0$  and  $f(x') < 0$  for some  $x, x' \in \mathbb{R}^n$ .

We are interested in the case  $n = 2$  and  $a_{ij} \in \mathbb{Z}$ .

**Lemma 4.4.** Let  $f(x, y) = ax^2 + bxy + cy^2$  be a BQF which has discriminant  $d = b^2 - 4ac$ .

- (i) If  $d < 0$  and  $a > 0$ , then  $f$  is positive definite.
- (ii) If  $d < 0$  and  $a < 0$ , then  $f$  is negative definite.
- (iii) If  $d > 0$ , then  $f$  is indefinite.
- (iv) If  $d = 0$ , then  $f = \lambda(mx + ny)^2$  for  $\lambda, m, n \in \mathbb{Z}$ .

*Proof.*

$$\begin{aligned} 4af(x, y) &= 4a^2x^2 + 4abxy + 4acy^2 = \\ &= (2ax + by)^2 + (4ac - b^2)y^2 = (2ax + by)^2 - dy^2. \end{aligned}$$

(i) and (ii): If  $d < 0$  and  $a \neq 0$ , then it follows that  $4af(x, y) \geq 0$  with equality if and only if  $x = y = 0$ . The cases  $a > 0$  and  $a < 0$  now show  $f$  is either positive or negative definite as desired.

(iii): Suppose  $d > 0$ . If  $a \neq 0$ , then the above equation shows us that  $4af(1, 0) > 0$  and  $4af(-b, 2a) < 0$ , so  $f$  is indefinite.

If  $a = 0$ , then replace  $f(x, y) \mapsto f(y, x)$ . This works unless  $a = c = 0$ , but then  $b \neq 0$ , so  $f(x, y) = bxy$ , which is obviously indefinite.

(iv): Omitted (not interesting nor difficult). □

**Remark.** It is possible for a BQF  $(a, b, c)$  with  $a, b, c > 0$  to be indefinite, e.g.  $(1, 3, 1)$ .

It is also possible for  $(a, b, c)$  with  $b < 0$  to be positive definite, e.g.  $(1, -1, 2)$ .

From now on, we will concentrate on positive definite BQFs, i.e. forms  $(a, b, c)$  with  $d = b^2 - 4ac < 0$  and  $a > 0$  (and hence  $c > 0$ ).

We have an equivalence relation  $\sim$  on positive definite BQFs, and we want to study the equivalence classes. It will help if we can specify a "simplest" form for each equivalence class.

**Example 4.3.** Consider  $(10, 34, 29)$ . The middle coefficient is large – can we decrease it? If  $f(x) = ax^2 + bxy + cy^2$ , then one substitution we may try is

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

Taking  $\lambda = \pm 1$  shows

$$(a, b, c) \sim (a, b \pm 2a, a \pm b + c). \quad (\dagger)$$

In our example, we get  $(10, 34, 29) \sim (10, 14, 5) \sim (10, -6, 1)$ .

Making the substitution  $X = y, Y = -x$  gives

$$(a, b, c) \sim (c, -b, a). \quad (\ddagger)$$

In our example we now get

$$(10, -6, 1) \sim (1, 6, 10) \sim (1, 4, 5) \sim (1, 2, 2) \sim (1, 0, 1).$$

**Remark.** It is a good idea to check that the discriminant doesn't change (to catch mistakes).

**Remark.** We can ensure  $|b| \leq a$  via  $(\dagger)$ , and  $a \leq c$  via  $(\ddagger)$ .

**Definition 4.6.** A positive definite BQF is **reduced** if either

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

(Think of this as  $|b| \leq a \leq c$  with some extra conditions).

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

*Proof.* We have operations

$$S : (a, b, c) \mapsto (c, -b, a), \quad T_{\pm} : (a, b, c) \mapsto (a, b \pm 2a, a \pm b + c).$$

If  $a > c$ , then use  $S$  to decrease  $a$  while leaving  $|b|$  unchanged. If  $a \leq c$  and  $|b| > a$ , then use  $T_{\pm}$  to decrease  $|b|$  while leaving  $a$  unchanged.

Repeat these steps. Each step decreases  $a + |b|$ , so this procedure must eventually reach a form with  $|b| \leq a \leq c$ . Finally, to get the form we want in the lemma:

- If  $b = -a$ , then apply  $T_+$  to replace  $(a, -a, c) \mapsto (a, a, c)$ .
- If  $a = c$  and  $b < 0$ , then apply  $S$  to get  $b > 0$ .

□

**Lemma 4.6.** Let  $f = (a, b, c)$  be a reduced positive definite BQF with discriminant  $d$ . Then  $|b| \leq a \leq \sqrt{\frac{|d|}{3}}$  and  $b \equiv d \pmod{2}$ .

*Proof.* Being reduced implies  $|b| \leq a \leq c$ , and  $d = b^2 - 4ac \leq ac - 4ac = -3ac \leq -3a^2 \implies a^2 \leq \frac{|d|}{3}$ . Also  $d = b^2 - 4ac \implies b \equiv d \pmod{2}$ .  $\square$

**Example 4.4.** Consider  $d = -4$ . We must have  $a = 1$  by the lemma above (as  $a > 0$ ), and  $b = 0$  (by parity), so solve for  $c$  to get  $c = 1$ , i.e.  $x^2 + y^2$  is the only positive definite reduced BQF with discriminant  $-4$ .

We can now return to the beginning of this section and answer our original question: which numbers can be written as the sum of two squares?

*Proof of Theorem 4.1 (continued).* Let  $p$  be a prime,  $p \equiv 1 \pmod{4}$ . We have  $\left(\frac{-1}{p}\right) = 1$ , so  $\exists u \in \mathbb{Z}$  such that  $u^2 \equiv -1 \pmod{p} \implies u^2 = -1 + kp$  for some  $k \in \mathbb{Z}$ . Let  $f = (p, 2u, k)$ , so  $\text{disc}(f) = 4u^2 - 4pk = -4$ .

By Lemma 4.5,  $f \sim g$  for some reduced form  $g$ , but by our above example,  $g(x, y) = x^2 + y^2$ . Now  $f$  represents  $p$  (take  $x = 1, y = 0$ ), so  $g$  also represents  $p$ , i.e.  $p$  is the sum of two squares as required.  $\square$

**Question.** Can reduced forms be equivalent?

**Definition 4.7.** Let  $f$  be a BQF and  $n \in \mathbb{Z}$ . We say  $f$  **represents**  $n$  if  $n = f(x, y)$  for some  $x, y \in \mathbb{Z}$ . We say  $f$  **properly represents**  $n$  if  $n = f(x, y)$  for some coprime  $x, y \in \mathbb{Z}$ .

**Remark.** Equivalent forms properly represent the same integers, since if  $X = \alpha x + \gamma y, Y = \beta x + \delta y$  with  $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ , then  $\alpha\delta - \beta\gamma = 1$  implies  $\gcd(X, Y) = 1 \iff \gcd(x, y) = 1$ .

**Lemma 4.7.** The smallest integers properly represented by a reduced positive definite BQF  $f = (a, b, c)$  are  $a, c, a - |b| + c$  in that order.<sup>1</sup>

*Proof.*  $f$  reduced  $\implies |b| \leq a \leq c \implies a \leq c \leq a - |b| + c$ . We have  $f(1, 0) = a, f(0, 1) = c$ . If  $x = 0$ , then  $\gcd(x, y) = 1 \implies y = \pm 1$ . Likewise, if  $y = 0$ , then  $x = \pm 1$ .

So it remains to show that the smallest number represented by  $f$  using nonzero  $x, y$  is  $a - |b| + c$ . But if  $|x| \geq |y| \geq 1$ , then

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

We can achieve equality with  $f(1, \pm 1)$ . We proceed similarly if  $|y| \geq |x| \geq 1$ .  $\square$

<sup>1</sup>Values on this list are repeated if they are represented in more than one way, not counting repeats of the form  $f(x, y) = f(-x, -y)$ .



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

*Proof.* Existence follows from Lemma 4.5.

Uniqueness: Suppose  $f = (a, b, c)$  and  $g = (a', b', c')$  are equivalent reduced BQFs. We want to show  $a = a', b = b', c = c'$ . By Lemma 4.7,  $a = a', c = c'$  and  $a - |b| + c = a' - |b'| + c'$ , so  $(a, b, c) = (a', \pm b', c')$ .

If  $b = 0$ , we're done. If  $b \neq 0$ , can  $(a, b, c)$  and  $(a, -b, c)$  both be reduced? If yes, then  $a < c$  (since  $a = c$  requires  $b \geq 0$  by definition) and  $|b| < a$  (since we can't have  $b = -a$ ). Hence  $a < c < a - |b| + c$ . By Lemma 4.7 again,  $f(x, y) = a \iff (x, y) = (\pm 1, 0)$  and  $f(x, y) = c \iff (x, y) = (0, \pm 1)$ , and likewise for  $g$ .

Suppose  $g(x, y) = f(\alpha x + \gamma y, \beta x + \delta y) = f(X, Y)$ . Then

$$(X, Y) = (\pm 1, 0) \iff (x, y) = (\pm 1, 0)$$

$$(X, Y) = (0, \pm 1) \iff (x, y) = (0, \pm 1),$$

i.e.  $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ . But  $\alpha\delta - \beta\gamma = 1$ , so  $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ , so  $f = g$  as required.  $\square$

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

01 Nov 2022,  
Lecture 12

**Example 4.5.** Consider  $d = -24$ . We want to find  $f = (a, b, c)$  reduced with  $b^2 - 4ac = -24$ . By Lemma 4.6,  $|b| \leq a \leq \sqrt{8}$  and  $b$  is even.

- If  $a = 1$ , then  $b = 0$  and hence  $c = 6 \implies (1, 0, 6)$ . We can check that this is reduced.
- If  $a = 2$ , then  $c = \frac{b^2 + 24}{8}$ .
  - If  $b = 0$ , then  $c = 3$ . This is reduced.
  - If  $b = \pm 2$ , then  $c \notin \mathbb{Z}$ .

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

More generally, Lemma 4.6 shows that for every  $d$ , there are only finitely many reduced forms with discriminant  $d$ .

**Definition 4.8.** The **class number** of  $d$ , denoted  $h(d)$  is the number of equivalence classes of positive definite BQFs with discriminant  $d$ .

By Theorem 4.8, this is the number of reduced forms with discriminant  $d$ , hence finite by the last remark.

**Example 4.6.** As we have already seen,  $h(-4) = 1, h(-24) = 2$ .

**Definition 4.9.**  $d \equiv 0, 1 \pmod{4}$  is a **fundamental discriminant** if it is not of the form  $d = k^2 d_1$  for some integer  $k \geq 1$  and  $d_1 \equiv 0, 1 \pmod{4}$ .

Aside:

**Remark.** Let  $d < 0$  be a fundamental discriminant. Gauss defined a group law on the set of equivalence classes of positive definite BQFs with discriminant  $d$ . The abelian group obtained in this way is the same as the class group of the field  $\mathbb{Q}(\sqrt{d})$  (see Part II Number Fields). We insisted that  $\alpha\delta - \beta\gamma = 1$  in the definition of equivalence (not just  $= \pm 1$ ), since otherwise inverse elements in the class group would be the same element, hence it is no longer a group. End of aside.

**Some theorems about class numbers.**

(i) (Mertens 1874).

$$\sum_{-X < d < 0} h(d) \sim \frac{\pi}{18} X^{\frac{3}{2}} \text{ as } X \rightarrow \infty.$$

(ii) (Heilbronn 1934)  $h(d) \rightarrow \infty$  as  $|d| \rightarrow \infty$ .

(iii) (Siegel 1935) For every  $\epsilon > 0$ ,  $\exists c > 0$  such that  $h(d) > c|d|^{\frac{1}{2}-\epsilon}$ .

(iv) (Baker-Stark 1967)  $h(d) = 1 \iff d \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$ .

End of aside.

**Lemma 4.9.** Let  $f$  be a BQF and  $n \in \mathbb{Z}$ . Then  $f$  properly represents  $n$  if and only if  $f$  is equivalent to a form with first coefficient  $n$ .

*Proof.*  $\Leftarrow$  : Suppose  $f \sim g(n, b, c)$ . Then  $g(1, 0) = n \implies g$  properly represents  $n$ , so  $f$  properly represents  $n$ .

$\implies$  :  $f(\alpha, \beta) = n$  for some  $\alpha, \beta \in \mathbb{Z}$  coprime. By Euclid's algorithm,  $\exists \gamma, \delta \in \mathbb{Z}$  such that  $\alpha\delta - \beta\gamma = 1$ . Then  $f$  is equivalent to  $g(x, y) = f(\alpha x + \gamma y, \beta x + \delta y)$  with first coefficient  $g(1, 0) = f(\alpha, \beta) = n$ .  $\square$

**Theorem 4.10.** Let  $n$  be a positive integer and  $d < 0$  a discriminant. Then  $n$  is properly represented by some positive definite BQF with discriminant  $d$  if and only if the congruence

$$x^2 \equiv d \pmod{4n}$$

is soluble.

*Proof.*  $\implies$  : Lemma 4.9 shows  $f \sim g$  with  $g = (n, b, c)$ . Then

$$d = \text{disc}(f) = \text{disc}(g) = b^2 - 4nc \equiv b^2 \pmod{4n}.$$

$\Leftarrow$  : We are given  $b, c \in \mathbb{Z}$  such that  $b^2 = d + 4nc$ . Then  $f = (n, b, c)$  is a form of discriminant  $d$  and it properly represents  $n$  (with  $x = 1, y = 0$ ).  $\square$

**Example 4.7.** Which integers are properly represented by  $f(x, y) = x^2 + xy + 2y^2$ ?

We have  $\text{disc}(f) = -7$ , so  $f$  is positive definite. By Lemma 4.6, any reduced form with discriminant  $-7$  satisfies  $|b| \leq a \leq 1$  and  $b$  is odd. Hence  $(a, b, c) = (1, 1, 2)$  or  $(a, b, c) = (-1, -1, 2)$ . But the second one is not reduced, hence  $h(-7) = 1$  and all positive definite BQFs with discriminant  $-7$  are equivalent.

Hence  $n$  is properly represented by  $x^2 + xy + 2y^2$  if and only if  $x^2 \equiv -7 \pmod{4n}$  is soluble.

Assume  $n = p$  is prime and  $p \neq 2, 7$ . By CRT, the above is equal to

03 Nov 2022,  
Lecture 13

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

$$\text{But } \left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} \left(\frac{p}{7}\right) = \left(\frac{p}{7}\right).$$

We conclude that  $p = x^2 + xy + 2y^2$  for some  $x, y \in \mathbb{Z}$  means that  $p \equiv 1, 2, 4 \pmod{7}$  or  $p = 7$  (we check  $p = 2, 7$  separately).

**Lemma 4.11.** Let  $p$  be an odd prime and  $a \in \mathbb{Z}$ . If  $\left(\frac{a}{p}\right) = 1$ , then the congruence  $x^2 \equiv a \pmod{p^n}$  is soluble  $\forall n \geq 1$ .

*Proof.* Induction on  $n$ . The case  $n = 1$  is clear.

Now let  $n \geq 1$  and suppose  $x^2 \equiv a \pmod{p^n}$ , i.e.  $x^2 = a + kp^n, k \in \mathbb{Z}$ . For  $t \in \mathbb{Z}$ , we have  $(x + tp^n)^2 \equiv x^2 + 2xtp^n \equiv a + (2xt + k)p^n \pmod{p^{n+1}}$ . Now we have  $(2x, p) = 1$ , so we can solve  $2xt + k \equiv 0 \pmod{p}$ , so we're done.  $\square$

**Remark.** A similar argument shows that  $a \in \mathbb{Z}$  with  $a \equiv 1 \pmod{8}$ , then  $x^2 \equiv a \pmod{2^n}$  is soluble  $\forall n \geq 1$ .

**Above example continued:** Write  $n = 2^\alpha 7^\beta p_1^{\gamma_1} \dots p_r^{\gamma_r}$  for  $p_i$  distinct powers. Then

$$x^2 \equiv -7 \pmod{4n} \text{ is soluble} \iff \begin{cases} x^2 \equiv -7 \pmod{2^{\alpha+2}} \text{ is soluble.} \\ x^2 \equiv -7 \pmod{7^{\beta+1}} \text{ is soluble.} \\ x^2 \equiv -7 \pmod{p_i^{\gamma_i}} \text{ is soluble } \forall 1 \leq i \leq r. \end{cases}$$

The first condition is always true by the remark above. The second one has no solutions mod 49, so hence  $\beta \leq 1$ . For the last condition, use the above lemma to get that we need  $\left(\frac{-7}{p_i}\right) = 1 \forall 1 \leq i \leq r$ .

Hence we want  $7^2 \nmid n$  and all primes  $p \mid n$  with  $p \neq 7$  satisfy  $p \equiv 1, 2, 4 \pmod{7}$ .

The integers represented by  $x^2 + xy + y^2$  (not necessarily properly) are then of the form  $k^2 n$  for  $k \in \mathbb{Z}$  and  $n$  as described above.

**Conclusion.**  $n = x^2 + xy + 2y^2$  for some  $x, y \in \mathbb{Z} \iff$  every prime  $p \equiv 3, 5, 6$  which divides  $n$  divides it to an even power.

**Remarks.**

- (i) If  $h(d) = 1$ , we have shown how to solve the problem of which integers are represented by a given form of discriminant  $d < 0$ .

If  $h(d) > 1$ , we can determine which integers are represented by *some* form of discriminant  $d$ . For some values of  $d$  we can still distinguish which forms represent which numbers using congruence conditions.

- (ii) What about quadratic forms in more variables?

**Theorem 4.12** (Lagrange 1770). Every positive integer is a sum of four squares.

**Theorem 4.13** (Legendre 1797). A positive integer  $n$  is a sum of 3 squares if and only if  $n \neq 4^a(8b+7)$  for some integers  $a, b \geq 0$ .

- (iii) A geometric way to think about reduction: Let  $f(x, y) = ax^2 + bxy + cy^2$  be a positive definite BQF, so  $d = b^2 - 4ac < 0$ . Let  $\tau \in \mathbb{C}$  with  $f(\tau, 1) = 0$  and  $\text{Im}(\tau) > 0$ , so  $\tau = \frac{-b \pm \sqrt{|d|i}}{2a}$ , and  $|\tau|^2 = \frac{b^2 - d}{4a^2} = \frac{c}{a}$ .

So  $|b| \leq a \leq c \iff |\text{Re}(\tau)| \leq \frac{1}{2}$  and  $|\tau| \geq 1$ . Let  $\mathcal{F}$  be this subregion of  $\mathbb{C}$ . Then  $SL_2(\mathbb{Z}) \subset SL_2(\mathbb{R})$  acts on  $\mathcal{H} = \{\tau \in \mathbb{C} \mid \text{Im}(\tau) > 0\}$  via  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \tau \mapsto \frac{a\tau + b}{c\tau + d}$ , and the operations  $S$  and  $T_\pm$  in the proof of Lemma 4.5 correspond to the Möbius maps  $S : \tau \mapsto \frac{-1}{\tau}$  and  $T_\pm : \tau \mapsto \tau \pm 1$ . So we just start somewhere in the complex plane and apply these transformations until we end up in  $\mathcal{F}$ .

- (iv) Extra conditions in the definition of a reduced form correspond to conditions concerning the boundary of  $\mathcal{F}$ .