MA257 Introduction to Number Theory

Lecture notes

Sam Chow

University of Warwick, January to March 2024

Contents

This is a course in elementary number theory. There'll be opportunities to learn more advanced techniques in MA3A6 Algebraic Number Theory, MA4L6 Analytic Number Theory, MA426 Elliptic Curves, and MA4H9 Modular Forms.

1 Divisibility and congruences

Recall the set of positive integers

$$\mathbb{N} = \{1, 2, \ldots\}.$$

The integers form a ring

$$\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\},$$

and the rationals form a field

$$\mathbb{Q} = \{a/b : a, b \in \mathbb{Z}, b \neq 0\}.$$

Given $a, b \in \mathbb{Z}$, we say that a *divides* b, and write $a \mid b$, if there exists an integer c such that $ac = b$. Alternatively, we say that a is a *divisor* of b, or that b is a *multiple* of a, or that b is *divisible by* a. We write $a \nmid b$ if a does not divide b.

Example 1.0.1. We have $2 \mid 6$ and $0 \mid 0$.

Lemma 1.0.2 (Division algorithm, a.k.a. division with remainder)**.** *Let $a \in \mathbb{N}$ and $b \in \mathbb{Z}$. Then there exist unique integers q, r such that*

$$b = qa + r, \qquad 0 \leqslant r < a.$$

We call q the *quotient* and r the *remainder*.

Example 1.0.3. 42 is not a multiple of 10, as there's a remainder:

$$42 = 4 \times 10 + 2.$$

Proof. For existence, let $q = \lfloor b/a \rfloor$ be the greatest integer $q \leqslant b/a$, and put $r = b - aq$. Then

$$b/a - 1 < q \leqslant b/a,$$

so

$$r \geqslant b - ab/a = 0$$

and

$$r < b - a(b/a - 1) = a.$$

For uniqueness, suppose

$$b = aq + r = aq_1 + r_1, \qquad 0 \leqslant r, r_1 < a.$$

Then a divides $r - r_1$ and $|r - r_1| < a$, whence $r = r_1$ and $q = q_1$. □

An integer $n > 1$ is *prime* if its only positive divisors are 1 and n, and *composite* if it's not prime. The integer 1 is neither prime nor composite.

Example 1.0.4 (Grothendieck prime)**.** What are the prime divisors of 57?

Sieve of Eratosthenes (algorithm):

1. Write down integers from 2 to N in natural order.
2. Strike out all multiples of 2 (except 2).
3. Find the next remaining number (the one that is not struck out), call it R.
4. If $R \leqslant \sqrt{N}$ then strike out all multiples of R (except R) and go to step 3, otherwise stop the algorithm (the remaining numbers in the list are all the primes $\leqslant N$).

Example 1.0.5. Let's use this to list the primes up to 50 (in class).

Theorem 1.0.6 (Euclid, circa 300BC)**.** *There are infinitely many primes.*

Proof. Assume for a contradiction that $p_1, \ldots, p_n$ are all of the primes. Then

$$p_1 \cdots p_n + 1$$

is indivisible by $p_1, \ldots, p_n$, since the remainder is 1. However, strong induction assures us that any integer greater than 1 has a prime divisor. □

1.1 Euclid's algorithm

Given integers a and b, not both zero, we write $\gcd(a, b)$ or (a, b) for the greatest common divisor of a and b.

Example 1.1.1. Very inefficiently: the positive divisors of 12 are 1, 2, 3, 4, 6, 12, so $\gcd(12, 20) = 4$.

Is there an efficient way, especially for large values?

Example 1.1.2. Suppose we want to find $\gcd(2024, 70)$. We have

$$\begin{aligned} 2024 &= 28 \times 70 + 64 \\ 70 &= 64 + 6 \\ 64 &= 10 \times 6 + 4 \\ 6 &= 4 + \mathbf{2} \\ 4 &= 2 \times 2, \end{aligned}$$

so the GCD is 2.

We may assume that $0 < a \leqslant b$, since $(0, b) = b$.

1. Put $a_0 = a$ and $b_0 = b$.
2. Use the division algorithm to find $q_0, r_0 \in \mathbb{Z}$ such that $b_0 = q_0 a_0 + r_0$ and $0 \leqslant r < a_0$.
3. If $r_0 = 0$ then $\gcd(a, b) = a_0$.
4. If $0 < r_0 < a_0$, then set $a_1 = r_0$ and $b_1 = a_0$, and repeat the process.

Proof. The $a_i \in \mathbb{Z}_{\geqslant 0}$ are decreasing, so the algorithm must terminate.

If $b = aq + r$, then the common divisors of r and a are the same as the common divisors of a and b, so $\gcd(r, a) = \gcd(a, b)$. If the algorithm terminates after $i + 1$ steps, then

$$a_i = \gcd(0, a_i) = \gcd(a_i, a_{i-1}) = \cdots = \gcd(a_1, a_0) = \gcd(a, b).$$

□

Euclid's algorithm is efficient, in that it only takes polynomially many steps in terms of the input size $\log a$. If one were to test possible divisors of a, starting from 2 and stopping when one is found, then the time taken would be exponential. The latter is called *trial division*. There's also a version where only primes are tested for divisibility.

The algorithm can be run backwards to express the GCD as a linear combination of the two numbers. This is called the *extended Euclidean algorithm*.

Example 1.1.3. We have

$$\begin{aligned} 2 &= 6 - 4 \\ &= 6 - (64 - 10 \times 6) = 11 \times 6 - 64 \\ &= 11(70 - 64) - 64 = 11 \times 70 - 12 \times 64 \\ &= 11 \times 70 - 12(2024 - 28 \times 70) = 347 \times 70 - 12 \times 2024. \end{aligned}$$

This gives a practical way to establish the fundamental result below.

Lemma 1.1.4 (Bézout's lemma)**.** *Let a and b be integers, not both zero. Then there exist $x, y \in \mathbb{Z}$ such that*

$$ax + by = \gcd(a, b).$$

Corollary 1.1.5. *Let a and b be integers, not both zero, and let $d \in \mathbb{Z}$. Then d divides a and b if and only if $d \mid \gcd(a, b)$.*

Proof. If d divides $\gcd(a, b)$ then it divides a and b.

Conversely, suppose d divides a and b. For some $x, y \in \mathbb{Z}$, we have

$$\gcd(a, b) = ax + by,$$

which is divisible by d. □

1.2 The fundamental theorem of arithmetic

Lemma 1.2.1 (Euclid's lemma)**.** *Let $m, n \in \mathbb{Z}$, and let p be a prime dividing mn. Then p divides m or n.*

Proof. Suppose $p \nmid m$. Then $\gcd(p, m) = 1$, and Bézout's lemma furnishes integers x and y such that

$$mx + py = 1.$$

Now $n = n(mx + py)$ is divisible by p. □

It's necessary to assume that p is prime. Can you think of an example to demonstrate this necessity?

Theorem 1.2.2 (Fundamental theorem of arithmetic)**.** *Any positive integer is uniquely a product of primes.*

What's the prime factorisation of 2024?

Proof. Let $n \in \mathbb{N}$. We prove existence by strong induction. For $n = 1$, we use the empty product. For $n > 1$, we may assume that n is composite, so $n = ab$ for some integers a, b in the range $1 < a, b < n$. By our inductive hypothesis, the integers a and b are products of primes. Thus, so too is n.

For uniqueness, we also use strong induction. If $n = 1$ is expressed as a product of primes, then it must be the empty product, since any other product of primes is at least 2. Now suppose

$$2 \leqslant n = p_1 \cdots p_s = q_1 \cdots q_t$$

for some primes $p_1, \ldots, p_s$ and $q_1, \ldots, q_t$. By Euclid's lemma, the prime p_1 must divide some q_j, and therefore must equal q_j. By reordering the primes q_j, we may assume that $p_1 = q_1$. Now

$$p_2 \cdots p_s = q_2 \cdots q_t < n,$$

so by our inductive hypothesis we must have the multiset equality

$$\{\{p_2, \ldots, p_s\}\} = \{\{q_2, \ldots, q_t\}\}.$$

Finally, as $p_1 = q_1$, we have

$$\{\{p_1, \ldots, p_s\}\} = \{\{q_1, \ldots, q_t\}\}.$$

□

The *least common multiple* of $x, y \in \mathbb{Z}$, denoted $\operatorname{lcm}(x, y)$ or $[x, y]$, is the least positive integer that is a multiple of x and y.

Lemma 1.2.3. *Let $x, y \in \mathbb{N}$. Let $p_1, \ldots, p_k$ be the distinct primes dividing xy, and let*

$$x = p_1^{a_1} \cdots p_k^{a_k}, \qquad y = p_1^{b_1} \cdots p_k^{b_k}$$

be the prime factorisations of x and y, respectively. Then

$$(x, y) = \prod_{i \leqslant k} p_i^{m_i}, \qquad [x, y] = \prod_{i \leqslant k} p_i^{M_i},$$

where $m_i = \min\{a_i, b_i\}$ and $M_i = \max\{a_i, b_i\}$.

Proof. Exercise. □

Corollary 1.2.4. *If $x, y \in \mathbb{N}$ then*

$$(x, y)[x, y] = xy.$$

We can also consider the GCD or LCM of more than two integers. What's $\operatorname{lcm}(1, 2, 3, 4, 5, 6, 7, 8, 9, 10)$?

Two (or more) integers are *coprime* (or *relatively prime*) if they don't have any prime factors in common, i.e. their GCD is 1. By Bézout's lemma, this happens if and only if 1 can be expressed as a linear combination of the two integers. The following two useful lemmas can be proved either using either this characterisation or the fundamental theorem of arithmetic.

Lemma 1.2.5. *If $(a, m) = (b, m) = 1$ then $(ab, m) = 1$.*

Lemma 1.2.6 (General Euclid lemma)**.** *If $d \mid xy$ and $(d, x) = 1$ then $d \mid y$.*

Before moving on, we remark that number theory is sometimes done in situations where we don't have unique factorisation into irreducible elements.

Example 1.2.7. Unique factorisation into irreducible elements fails in the ring $\mathbb{Z}[\sqrt{-5}]$, since

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \times 3.$$

This is explored further in MA3A6 Algebraic Number Theory.

1.3 Fermat primes, Mersenne primes, and perfect numbers

Fermat claimed in a letter to have proved that the numbers

$$F_k = 2^{2^k} + 1 \qquad (k \geqslant 0)$$

are all prime. Whilst the first five of these are prime, namely

$$3, 5, 17, 257, 65537,$$

it's since been shown that $F_5, \ldots, F_{32}$ are composite. The numbers F_k are called *Fermat numbers*, and the prime ones are called *Fermat primes*.

For p prime, denote $M_p = 2^p - 1$. Primes of this form are called *Mersenne primes*. The largest known prime is $2^{82589933} - 1$, discovered as part of the Great Internet Mersenne Prime Search (GIMPS) programme.

The sum-of-divisors function is given by

$$\sigma_1(n) = \sum_{d|n} d,$$

where the sum is over positive divisors. A positive integer n is *perfect* if $\sigma_1(n) = 2n$.

Example 1.3.1. We have $6 = 3 + 2 + 1$, so 6 is perfect.

An *arithmetic function* is a function $\mathbb{N} \to \mathbb{C}$. An arithmetic function f is *multiplicative* if $f(mn) = f(m)f(n)$ holds for any coprime positive integers m and n.

Lemma 1.3.2. *The sum-of-divisors function is multiplicative.*

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

$$\sigma_1(mn) = \sum_{d|mn} d = \sum_{d_1|m} \sum_{d_2|n} d_1 d_2 = \sigma_1(m)\sigma_1(n).$$

□

Example 1.3.3. Let $M_p = 2^p - 1$ be a Mersenne prime, and put $n = 2^{p-1}M_p$. Then

$$\sigma_1(n) = \sigma_1(2^{p-1})\sigma_1(M_p) = (2^p - 1)2^p = 2n,$$

so n is perfect.

Theorem 1.3.4 (Euclid–Euler theorem)**.** *If $n \in \mathbb{N}$ is even then n is perfect if and only if*

$$n = 2^{p-1}M_p,$$

where $M_p = 2^p - 1$ is a Mersenne prime.

The proof is elementary, but let's move on. A famous open problem asks if there are any odd perfect numbers.

1.4 Congruences (modular arithmetic)

Let $m \in \mathbb{N}$. We say that integers x and y are *congruent modulo* m, and write $x \equiv y \bmod m$, if m divides $x - y$.

Example 1.4.1. Modular arithmetic is like going around a clock. 1700 hours is 5pm, because $17 \equiv 5 \bmod 12$.

Another way to think about it is that numbers are congruent modulo m if they leave the same remainder when divided by m. It's easy to check that this is an equivalence relation on $\mathbb{Z}$. The integers can thus be partitioned into congruence classes $r + m\mathbb{Z}$, where $0 \leqslant r < m$. These congruence classes form the quotient ring $\mathbb{Z}/m\mathbb{Z}$, which we'll soon discuss further.

Example 1.4.2. Modulo 10 is taking the last digit: $2024 \equiv 4 \bmod 10$.

Lemma 1.4.3 (Congruences respect addition and multiplication)**.** *Let $m \in \mathbb{N}$. Let a, b, α, β be integers such that*

$$a \equiv \alpha \bmod m, \qquad b \equiv \beta \bmod m.$$

Then

$$a + b \equiv \alpha + \beta \bmod m, \qquad ab \equiv \alpha\beta \bmod m.$$

Thus, if $f(x, y) \in \mathbb{Z}[x, y]$, then

$$f(a, b) \equiv f(\alpha, \beta) \bmod m.$$

Proof. Exercise. □

Lemma 1.4.4 (Cancellation with congruences)**.** *Let $m \in \mathbb{N}$, and let $a, x, y \in \mathbb{N}$ with*

$$ax \equiv ay \bmod m.$$

(a) If $a \mid m$ then

$$x \equiv y \bmod m/a.$$

(b) If $(a, m) = 1$ then

$$x \equiv y \bmod m.$$

Proof. (a) We have $a(x - y) = cm$ for some $c \in \mathbb{Z}$, so $x - y = cm/a$, whence $x \equiv y \bmod m/a$.

(b) As m divides $a(x-y)$ and $(a,m)=1$, the general Euclid lemma tells us that m divides $x-y$, so $x \equiv y \bmod m$.

□

Example 1.4.5.

$$\begin{aligned} 4x &\equiv 4y \bmod 6 \\ \Leftrightarrow 2x &\equiv 2y \bmod 3 \\ \Leftrightarrow x &\equiv y \bmod 3. \end{aligned}$$

Before proceeding further, we demonstrate some modular obstructions to the solubility of diophantine equations (equations where we look for integer solutions).

Lemma 1.4.6. *Squares are 0 or 1 modulo 4.*

Proof.

x	$x^2 \bmod 4$
0	0
1	1
2	0
3	1

□

Corollary 1.4.7. *One cannot express 2023 as a sum of two squares.*

We can't write 2023 as a sum of three squares either.

Lemma 1.4.8. *Let n be a positive integer of the form $n = 4^k m$, where $k \geqslant 0$ and $m \equiv 7 \bmod 8$. Then n is not a sum of three squares.*

Proof. By checking 0,1,2,3,4,5,6,7, we find that squares are 0,1, or 4 modulo 8. Thus, three squares cannot sum to 7 modulo 8, which solves the $k = 0$ case.

We now induct on k. Let $k \geqslant 1$, and assume the result for smaller values of k. Suppose for a contradiction that

$$x^2 + y^2 + z^2 = 4^k m,$$

for some $x, y, z \in \mathbb{Z}$. Then $x^2 + y^2 + z^2 \equiv 0 \bmod 4$. This is only possible for x, y, z are all even, since x^2 is 0 mod 4 if x is even and 1 mod 4 if x is odd. Writing

$$x = 2u, \qquad y = 2v, \qquad z = 2w$$

yields

$$u^2 + v^2 + w^2 = 4^{k-1}m,$$

contradicting our inductive hypothesis. □

The proof above is an example of *infinite descent*, where any triple (x, y, z) with the property of interest produces a smaller such triple. As an exercise, show that if x, y, z are integers, not all zero, then $x^2 + y^2 \neq 3z^2$.

1.5 Linear congruences

Let $m \in \mathbb{N}$. We say that $0, 1, \ldots, m-1$ form a *complete set of residues* modulo m, because they have exactly one representative from each congruence class. The ring $\mathbb{Z}/m\mathbb{Z}$ is $\{0, 1, \ldots, m-1\}$ equipped with addition and multiplication modulo m. It's easy to check that this is a commutative ring.

Example 1.5.1 (Associativity)**.** Let $a, b, c \in \{0, 1, \ldots, m-1\}$. Write

$$ab = q_1 m + r_1, \qquad bc = q_2 m + r_2$$

with $0 \leqslant r_1, r_2 < m$. Then

$$r_1 c \equiv abc \equiv a r_2 \bmod m,$$

whence $(ab)c = a(bc) \in \mathbb{Z}/m\mathbb{Z}$.

Next, we study the multiplicative group of units (invertible elements) modulo m, which we denote by $(\mathbb{Z}/m\mathbb{Z})^\times$.

Lemma 1.5.2. *Let $m \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then a is invertible modulo m if and only if* $\gcd(a, m) = 1$.

Example 1.5.3. We have $(\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\} \bmod 6$.

Proof. The integer a is invertible modulo m if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + my = 1$. By Bézout's lemma, such integers exist if $(a, m) = 1$, and conversely if such integers exist then a, m must be coprime. □

Hence $(\mathbb{Z}/m\mathbb{Z})^\times$ comprises the coprime residue classes modulo m. The *Euler totient function* φ counts the number of coprime residue classes:

$$\varphi(m) = \#\{a \in \{1, 2, \ldots, m\} : \gcd(a, m) = 1\}.$$

Therefore $|(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$.

Example 1.5.4. We have $\varphi(6) = 2$.

We'll later deduce a nice formula for $\varphi(m)$, which is also referred to as the *Euler phi function*.

Lemma 1.5.5. *If p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field, and*

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \ldots, p-1\} \bmod p$$

has order $\varphi(p) = p - 1$.

Proof. It's a commutative ring, and any non-zero element is invertible (being coprime to the modulus). □

We also denote this by $\mathbb{F}_p$. Note that if m is composite then $\mathbb{Z}/m\mathbb{Z}$ isn't a field, since any prime divisor of m is non-invertible. Let's also practise finding inverses.

Example 1.5.6. We have

$$1^2 \equiv 2 \times 4 \equiv 3 \times 5 \equiv 6^2 \equiv 1 \bmod 7.$$

Mod 13 (card game):

1. Each player is dealt a hand of cards, interpreted as residue classes modulo 13 (J = 11, Q = 12, K = 13), and two cards a_1, a_2 are placed into the centre.

2. Racing, a player can play either the $a_1 + a_2$ (sum), $a_1 a_2$ (product), $2a_2 - a_1$ (AP = arithmetic progression) or $a_2^2 a_1^{-1}$ (GP = geometric progression) as the card a_3, declaring which type of move they've played.

3. Play continues with cards a_2 and a_3 in place of a_1 and a_2, and so on, until somebody finishes and wins.

Example 1.5.7. GP: 7, J, and...? We have

$$11 \equiv 24 \equiv 4(-7) \equiv 9 \times 7 \bmod 13,$$

so the next card is

$$9 \times 11 \equiv 8.$$

We can determine all solutions to a given linear congruence using our knowledge of inverses.

Lemma 1.5.8 (Solving a linear congruence)**.** *Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$. Then:*

(a) There exists $x \in \mathbb{Z}$ solving $ax \equiv b \bmod m$ if and only if $\gcd(a, m) \mid b$.

(b) If $\gcd(a, m) \mid b$, and $x_0 \in \mathbb{Z}$ is a solution to $ax_0 \equiv b \mod m$, then all solutions are given by

$$x_0 + \frac{tm}{\gcd(a, m)} \qquad (t \in \mathbb{Z}).$$

Proof. Put

$$g = \gcd(a, m), \qquad a = ga', \qquad m = gm',$$

so that $(a', m') = 1$.

(a) If $x \in \mathbb{Z}$ and $ax \equiv b \bmod m$ then $b \equiv ax \equiv 0 \bmod g$.

Conversely, if $g \mid b$ then, writing $b = gb'$, our congruence becomes

$$a'x \equiv b' \bmod m'.$$

This has a solution because $(a', m') = 1$. It's given by b' times the inverse of a' modulo m'.

(b) If $t \in \mathbb{Z}$ and $x = x_0 + tm/g$ then

$$ax \equiv b + atm/g \equiv b \bmod m.$$

It remains to show that there aren't any other solutions.

If x solves the congruence then

$$a'x \equiv b' \equiv a'x_0 \bmod m',$$

so m' divides $x - x_0$ by the general Euclid lemma. Therefore $x = x_0 + tm'$ for some $t \in \mathbb{Z}$.

□

Example 1.5.9. Let's find all $x \in \mathbb{Z}$ such that $100x \equiv 26 \bmod 82$. We rewrite this as

$$50x \equiv 13 \bmod 41,$$

then as

$$9x \equiv 13 \bmod 41.$$

All solutions will be gotten from one solution (the unique solution modulo 41 is 13 times the inverse of 9). Since 9 and 41 are coprime, we can express 1 as a linear combination of them using the extended Euclidean algorithm:

$$\begin{aligned} 41 &= 4 \times 9 + 5 \\ 9 &= 5 + 4 \\ 5 &= 4 + 1, \end{aligned}$$

so

$$\begin{aligned} 1 &= 5 - 4 \\ &= 5 - (9 - 5) = 2 \times 5 - 9 \\ &= 2(41 - 4 \times 9) - 9 \\ &= 2 \times 41 - 9 \times 9. \end{aligned}$$

Now

$$13 = 26 \times 41 - 117 \times 9,$$

so -117 is a solution to the congruence, and so too is $3 \times 41 - 117 = 6$. Thus, all solutions are given by

$$x = 6 + 41t \qquad (t \in \mathbb{Z}).$$

We saw how to solve a single linear congruence. The Chinese remainder theorem enables us to solve a system of linear congruences with pairwise coprime moduli.

Theorem 1.5.10 (Classical Chinese remainder theorem)**.** *Let $m_1, \ldots, m_K \in \mathbb{N}$ be pairwise coprime, and let $a_1, \ldots, a_K \in \mathbb{Z}$. Then there exists $x \in \mathbb{Z}$, unique modulo $\prod_k m_k$, such that*

$$x \equiv a_k \bmod m_k \qquad (1 \leqslant k \leqslant K).$$

This is given by $\sum_i a_i M_i y_i$, where $M_i = \prod_{j \neq i} m_j$ and $M_i y_i \equiv 1 \bmod m_i$.

Proof. For existence, observe that for each k we have

$$\sum_i a_i M_i y_i \equiv a_k M_k y_k \equiv a_k \bmod m_k.$$

For uniqueness, observe that if x, y are solutions then $x - y$ is divisible by $m_1, \ldots, m_K$. As the m_i are pairwise coprime, it follows from the fundamental theorem of arithmetic that $m_1 \cdots m_K$ divides $x - y$. □

Example 1.5.11. Consider the simultaneous congruences

$$x \equiv 1 \bmod 3, \qquad x \equiv 2 \bmod 5, \qquad x \equiv 3 \bmod 7.$$

The general solution is

$$x = x_0 + 105t \qquad (t \in \mathbb{Z}),$$

where

$$x_0 = M_1 y_1 + 2M_2 y_2 + 3M_3 y_3.$$

Here

$$M_1 = 35, \qquad M_2 = 21, \qquad M_3 = 15$$

and

$$35y_1 \equiv 1 \bmod 3, \qquad 21y_2 \equiv 1 \bmod 5, \qquad 15y_3 \equiv 1 \bmod 7.$$

Hence

$$2y_1 \equiv 1 \bmod 3, \qquad y_2 \equiv 1 \bmod 5, \qquad y_3 \equiv 1 \bmod 7,$$

so $y_1 \equiv -1 \bmod 3$ and finally

$$x_0 = -35 + 2 \times 21 + 3 \times 15 = -35 + 42 + 45 = 52.$$

All solutions are therefore given by $x = 52 + 105t$, for $t \in \mathbb{Z}$.

There was a clever way to find this from the beginning. Can you spot it?

There's also a version to do with finite groups.

Example 1.5.12. Since $3 \nmid 5$, how does $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ fit into the classification of finite abelian groups? Recall that this asserts that any finite abelian group is isomorphic to some $\prod_{k \leqslant K} \mathbb{Z}/d_k\mathbb{Z}$, where $d_1 \mid d_2 \mid \cdots \mid d_K$.

A *ring homomorphism* is a function between rings $f : R \to S$ such that $f(1) = 1$ and

$$f(x+y) = f(x) + f(y), \quad f(xy) = f(x)f(y) \qquad (x, y \in \mathbb{R}).$$

As an exercise, show that $f(0) = 0$.

Example 1.5.13. Reducing modulo m is a ring homomorphism $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

If f is a bijective ring homomorphism, then its inverse is a ring homomorphism, and we call f a ring *isomorphism*.

Theorem 1.5.14 (Algebraic Chinese remainder theorem)**.** *Let $m_1, \ldots, m_K \in \mathbb{N}$ be pairwise coprime, and put $M = \prod_k m_k$. Then*

$$\begin{aligned} \psi : \mathbb{Z}/M\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_K\mathbb{Z} \\ x &\mapsto (x \bmod m_1, \ldots, x \bmod m_K) \end{aligned}$$

is a ring isomorphism. Moreover, it restricts to a group isomorphism

$$(\mathbb{Z}/M\mathbb{Z})^\times \to (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_K\mathbb{Z})^\times.$$

Proof. Well-defined: if $x \in \mathbb{Z}$ then

$$x + M \equiv x \bmod m_k \qquad (1 \leqslant k \leqslant K).$$

We saw that modular arithmetic respects addition and multiplication, so ψ is a ring homomorphism. The classical Chinese remainder theorem defines an inverse function, so ψ is bijective and is therefore an isomorphism.

For the second part, note that $x \in \mathbb{Z}/M\mathbb{Z}$ is coprime to M if and only if it's coprime to each m_k. Therefore ψ restricts to a bijection

$$(\mathbb{Z}/M\mathbb{Z})^\times \to (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_K\mathbb{Z})^\times.$$

This is a group homomorphism because ψ is a ring homomorphism. Hence it's a group isomorphism. □

Recall that an *arithmetic function* is a function $\mathbb{N} \to \mathbb{C}$, and that an arithmetic function f is *multiplicative* if $f(mn) = f(m)f(n)$ holds for any coprime positive integers m and n.

Corollary 1.5.15. *Euler's totient function is multiplicative.*

Proof. Apply the algebraic CRT with $K = 2$. □

Lemma 1.5.16. *For $n \in \mathbb{N}$, we have*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product is over primes dividing n.

Proof. Observe that $\varphi(1) = 1$. Next, suppose $n = p^k$, for some prime p and some $k \in \mathbb{N}$. Then $\varphi(n)$ is the number of residue classes that aren't divisible by p, which is

$$p^k - p^{k-1} = p^k(1 - 1/p).$$

Finally, suppose $n = p_1^{k_1} \cdots p_r^{k_r}$, where the p_i are pairwise distinct primes and the k_i are positive integers. Then

$$\varphi(n) = \prod_{i \leqslant r} \varphi(p^{k_i}) = \prod_{i \leqslant r} p^{k_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

□

Example 1.5.17. We have

$$\varphi(20) = 20(1 - 1/2)(1 - 1/5) = 10 \times 4/5 = 8.$$

Here's another nice property, which is sometimes used in analytic number theory. The proof is instructive: to show that two multiplicative functions are equal, it suffices to compare them at prime powers.

Lemma 1.5.18 (Totient function identity)**.** *For $n \in \mathbb{N}$, we have*

$$\sum_{d|n} \varphi(d) = n,$$

where the sum is over the positive divisors of n.

Proof. We proceed in two steps. First, we show that the arithmetic function

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

is multiplicative. Let m and n be coprime positive integers. Then the positive divisors of mn are the numbers of the form de, where d, e are positive divisors of m, n respectively, and moreover $(d, e) = 1$ here. Thus

$$f(mn) = \sum_{d|m} \sum_{e|n} \varphi(de) = \sum_{d|m} \sum_{e|n} \varphi(d)\varphi(e) = f(m)f(n),$$

so f is indeed multiplicative.

It remains to prove that $f(p^k) = p^k$ for any prime power p^k. We compute that

$$f(p^k) = \sum_{j=0}^{k} \varphi(p^j) = 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) = p^k.$$

□

1.6 Standard congruences

Example 1.6.1 (Fast powering)**.** Let's compute 2^{200} mod 13. We have

$$200 = 128 + 64 + 8.$$

t	2^t mod 13
4	3
8	9
16	3
32	9
64	3
128	9

Using our table, we have

$$2^{200} = 2^{128}2^{64}2^8 \equiv 9 \times 3 \times 9 \equiv 9 \bmod 13.$$

Theorem 1.6.2 (Euler's theorem, 1760)**.** *Let $m \in \mathbb{N}$, and let $a \in \mathbb{Z}$ be coprime to m. Then*

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

Proof. Reducing modulo m, we have $x := \bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$. By Lagrange's theorem, its order k divides the order of the group, whence

$$x^{\varphi(m)} = (x^k)^{\varphi(m)/k} = 1.$$

□

Example 1.6.3. We have $3^{40} \equiv 1 \bmod 100$. What about 2^{40}?

Corollary 1.6.4 (Fermat's little theorem, 1640)**.** *Let p be prime, and let $a \in \mathbb{Z}$.*

(a) If $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$.

(b) We have $a^p \equiv a \bmod p$.

Proof. (a) Apply Euler's theorem.

(b) If $p \nmid a$, then apply (a) and multiply both sides by a. If $p \mid a$, then both sides are zero.

□

It follows that if $(a, n) = 1$ and $a^{n-1} \not\equiv 1 \bmod n$ then n is composite. The converse, however, is false. A *Carmichael number* is a composite number n such that if $a \in \mathbb{Z}$ and $(a, n) = 1$ then $a^{n-1} \equiv 1 \bmod n$. The smallest Carmichael number is $561 = 3 \times 11 \times 17$.

Example 1.6.5. Suppose x is coprime to 561. Then

$$\begin{aligned} x^{560} &= (x^2)^{280} \equiv 1 \bmod 3, \\ x^{560} &= (x^{10})^{56} \equiv 1 \bmod 11, \\ x^{560} &= (x^{16})^{35} \equiv 1 \bmod 17, \end{aligned}$$

by Fermat, so CRT gives $x^{560} \equiv 1 \bmod 561$.

The example above motivates a general criterion that we state below but won't formally prove. An integer is *squarefree* if it isn't divisible by the square of any prime.

Theorem 1.6.6 (Korselt, 1899)**.** *A composite number n is Carmichael if and only if it's squarefree* ***and,*** *for every prime $p \mid n$, we have $(p-1) \mid (n-1)$.*

Example 1.6.7. As 2, 10, and 16 divide 560, we see that $561 = 3 \times 11 \times 17$ is Carmichael.

There are infinitely many Carmichael numbers, but they're much rarer than primes. Thus, if $n \in \mathbb{N}$ satisfies $a^{n-1} \equiv 1 \bmod n$ whenever $(a, n) = 1$, then it's very likely to be prime!

Before we come to Wilson's theorem, we require some information about roots of polynomials.

Lemma 1.6.8 (General roots lemma)**.** *Let p be prime, and let $f(x) \in \mathbb{F}_p[x]$ be a non-zero polynomial of degree d. Then f has at most d roots in $\mathbb{F}_p$.*

Proof. This is clear for $d = 0$, so let's assume that $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}_p$ and induct on the degree. By polynomial long division, we can find $q(x) \in \mathbb{F}_p[x]$ and $r \in \mathbb{F}_p$ such that

$$f(x) = (x - \alpha)q(x) + r, \qquad \deg(q) = d - 1.$$

Substituting $x = \alpha$ yields $r = 0$, so $f(x) = (x - \alpha)q(x)$. If $\beta \neq \alpha$ is a root of f, then it's a root of q. By our inductive hypothesis, the polynomial q has at most $d - 1$ roots in $\mathbb{F}_p$, so f has at most d roots. □

In full generality, polynomial long division uses coefficients in a field, e.g. one can't divide x^2 by $2x$ with remainder over the integers. However, when dividing by a monic polynomial, polynomial long division can be done over any commutative ring.

Example 1.6.9. When dividing $x^5 + 3$ by $x^2 + 3$ over $\mathbb{Z}$ (i.e. in $\mathbb{Z}[x]$), the quotient is $x^3 - 3x$ and the remainder is $9x + 3$ (done in class by polynomial long division).

An *integral domain* is a commutative ring such that if $xy = 0$ then $x = 0$ or $y = 0$.

Lemma 1.6.10. *Any subring of a field is an integral domain.*

Proof. Let R be a subring of a field, and let $x, y \in R$ with $x \neq 0$ and $xy = 0$. Then

$$y = x^{-1}0 = 0.$$

□

Lemma 1.6.8 holds over any integral domain, with the same proof. The ring $\mathbb{Z}/m\mathbb{Z}$ is only an integral domain if m is prime.

Example 1.6.11. In $\mathbb{Z}/6\mathbb{Z}$, the quadratic polynomial $(x-2)(x-3) = x(x-5)$ has four roots.

Theorem 1.6.12 (Wilson's theorem)**.** *If p is prime then*

$$(p-1)! \equiv -1 \bmod p.$$

Proof. The polynomials

$$x^{p-1} - 1, \qquad (x-1)(x-2)\cdots(x-p+1)$$

agree at $x = 1, 2, \ldots, p-1$, by Fermat's little theorem. Their difference has at least $p-1$ roots and degree at most $p-2$, so it must vanish identically. Thus

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1) \bmod p$$

for all $x \in \mathbb{Z}$, and specialising $x = 0$ gives

$$-1 \equiv (-1)^{p-1}(p-1)! \equiv (p-1)! \bmod p.$$

□

If $n \neq 4$ is composite, then it's not too hard to show that

$$(n-1)! \equiv 0 \bmod n.$$

The upshot is that Wilson's theorem is a valid test of primality, albeit not a very practical one.

1.7 Primitive roots

We now examine the structure of the group $(\mathbb{Z}/m\mathbb{Z})^\times$ of units modulo m. By the Chinese remainder theorem, it suffices to consider prime power moduli.

Let $m \in \mathbb{N}$, and let $a \in \mathbb{Z}$ be coprime to m. The *order* of a modulo m, denoted $\mathrm{ord}_m(a)$, is the least $k \in \mathbb{N}$ such that $a^k \equiv 1 \bmod m$. In other words, it's the order of $a \in (\mathbb{Z}/m\mathbb{Z})^\times$.

Lemma 1.7.1 (Order lemma)**.** *Let $m \in \mathbb{N}$, and let $a \in \mathbb{Z}$ be coprime to m. Then:*

(a) If $k \in \mathbb{N}$ then $a^k \equiv 1 \bmod m$ if and only if $\mathrm{ord}_m(a) \mid k$.

(b) We have $\mathrm{ord}_m(a) \mid \varphi(m)$.

(c) For $u \in \mathbb{N}$, we have

$$\mathrm{ord}_m(a^u) = \frac{\mathrm{ord}_m(a)}{(u, \mathrm{ord}_m(a))}.$$

Proof. (a) This is a special case of the result for finite groups. Reprove it as an exercise.

(b) Apply Euler's theorem and (a).

(c) Write

$$x = \mathrm{ord}_m(a), \qquad g = \gcd(u, x), \qquad x = gx', \qquad u = gu',$$

so that $(x', u') = 1$. Observe that $\mathrm{ord}_m(a^u)$ is the least $k \in \mathbb{N}$ such that $a^{ku} \equiv 1 \bmod m$, which is the least k for which $x \mid ku$. This is the least k such that $x' \mid ku'$, whence

$$\mathrm{ord}_m(a^u) = x' = \frac{x}{g} = \frac{\mathrm{ord}_m(a)}{(u, \mathrm{ord}_m(a))}.$$

□

Given $m \in \mathbb{N}$, a *primitive root modulo* m is $a \in \mathbb{Z}$ such that $\mathrm{ord}_m(a) = \varphi(m)$. Equivalently, the integer a is a primitive root if it generates $(\mathbb{Z}/m\mathbb{Z})^\times$, i.e.

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{1, a, a^2, \ldots, a^{\varphi(m)-1}\}.$$

What's a primitive root modulo 7?

If g is a primitive root modulo m, then any element of $(\mathbb{Z}/m\mathbb{Z})^\times$ can be written as g^t, for some unique $t \in \{0, 1, \ldots, \varphi(m) - 1\}$. There's a primitive root modulo m if and only if $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic. For which m does this happen? Try it out for $m \leqslant 9$. It's easy to be cyclic if you're small! We'll see that there usually isn't a primitive root.

Theorem 1.7.2. *If p is prime then there are precisely $\varphi(p-1)$ primitive roots modulo p.*

Proof. For $d \in \mathbb{N}$ dividing $p-1$, write

$$A(d) = \{x \in (\mathbb{Z}/p\mathbb{Z})^\times : \mathrm{ord}_p(x) = d\}, \qquad f(d) = |A(d)|.$$

Observe that

$$\sum_{d|(p-1)} f(d) = p - 1 = \sum_{d|(p-1)} \varphi(d),$$

wherein we've used the order lemma and the totient function identity. We show, *a fortiori*, that $f(d) = \varphi(d)$ for all $d \mid (p-1)$. By our observation, it suffices to prove that $f(d) \leqslant \varphi(d)$ for all $d \mid (p-1)$, and in particular we may assume that $f(d) > 0$.

Let $d \in \mathbb{N}$ divide $p-1$ with $f(d) > 0$, and let $a \in A(d)$. Then

$$1, a, a^2, \ldots, a^{d-1}$$

are distinct solutions to $x^d \equiv 1 \bmod p$, and by the general roots lemma they must be all of the solutions. Now

$$f(d) = \#\{t \in \{0, 1, \ldots, d-1\} : \mathrm{ord}_p(a^t) = d\}\} = \varphi(d),$$

by the order lemma. □

If g is a primitive root modulo p, then any element of $(\mathbb{Z}/p\mathbb{Z})^\times$ can be written as g^t, for some unique $t \in \{1, 2, \ldots, p-1\}$.

Example 1.7.3. Let's now prove Wilson's theorem using a primitive root $g \bmod p$. We can assume that p is odd. By Fermat's little theorem, we have

$$(p-1)! \equiv g^{1+2+\cdots+(p-1)} \equiv (g^{(p-1)/2})^p \equiv g^{(p-1)/2} \equiv -1 \bmod p.$$

Lemma 1.7.4. *Let g be a primitive root modulo an odd prime p, and let $t \in \mathbb{N}$. Then g^t is a primitive root modulo p if and only if $(t, p-1) = 1$.*

Proof. The order lemma gives

$$\mathrm{ord}_p(g^t) = \frac{\mathrm{ord}_p(g)}{(t, \mathrm{ord}_p(g))} = \frac{p-1}{(t, p-1)}.$$

□

Conjecture 1.7.5 (Artin's conjecture on primitive roots, 1927)**.** *Let $g \neq -1$ be a non-square integer. Then there are infinitely many primes p for which g is a primitive root.*

Let's now return to our question of which groups $(\mathbb{Z}/m\mathbb{Z})^\times$ are cyclic. We require some preparatory lemmas.

Lemma 1.7.6. *Let p be prime, and let $t < p$ be a positive integer. Then*

$$\binom{p}{t} \equiv 0 \bmod p.$$

Proof. We have

$$\binom{p}{t} = \frac{p!}{t!(p-t)!} \equiv 0 \bmod p.$$

□

Lemma 1.7.7 (Power-up lemma)**.** *Let p be a prime, and let $k \in \mathbb{N}$. Then*

$$a \equiv b \bmod p^k \Rightarrow a^p \equiv b^p \bmod p^{k+1}.$$

Proof. For some $c \in \mathbb{Z}$, we have $a = b + cp^k$. The binomial theorem gives

$$a^p = b^p + (cp^k)^p + \sum_{t=1}^{p-1} \binom{p}{t} b^t (cp^k)^{p-t} \equiv b^p \bmod p^{k+1}.$$

□

Corollary 1.7.8. *Let p be an odd prime, and let $k \geqslant 2$ be an integer. Then*

$$(1+ap)^{p^{k-2}} \equiv 1 + ap^{k-1} \bmod p^k \qquad (a \in \mathbb{Z}).$$

Proof. This is clear if $k = 2$, so let's assume the the congruence for a specific value of $k \geqslant 2$ and prove it with $k+1$ in place of k. Inserting the inductive hypothesis into the power-up lemma gives

$$(1+ap)^{p^{k-1}} = ((1+ap)^{p^{k-2}})^p \equiv (1+ap^{k-1})^p \bmod p^{k+1}.$$

The binomial theorem now yields

$$(1+ap)^{p^{k-1}} \equiv 1 + ap^k \bmod p^{k+1},$$

completing the induction. □

Corollary 1.7.9. *Let p be an odd prime, let $k \in \mathbb{N}$, and let $a \in \mathbb{Z}$ with $p \nmid a$. Then* $\operatorname{ord}_{p^k}(1+ap) = p^{k-1}$.

Proof. Clearly we may assume that $k \geqslant 2$. Then

$$(1+ap)^{p^{k-1}} \equiv (1+ap^{k-1})^p \equiv 1 \bmod p^k,$$

so the order divides p^{k-1}. It must be exactly p^{k-1}, since

$$(1+ap)^{p^{k-2}} \equiv 1+ap^{k-1} \not\equiv 1 \bmod p^k.$$

□

Theorem 1.7.10. *Let p be an odd prime, and let $k \in \mathbb{N}$. Then:*

(a) There exists a primitive root $g \in \mathbb{Z}$ modulo p such that $g^{p-1} \not\equiv 1 \bmod p^2$.

(b) Any such g is a primitive root modulo p^k.

Proof. (a) We know that there's a primitive root g modulo p. If $g^{p-1} \equiv 1 \bmod p^2$, then

$$(g+p)^{p-1} \equiv 1 + (p-1)g^{p-2}p \not\equiv 1 \bmod p^2.$$

(b) Let $n = \mathrm{ord}_{p^k}(g)$. By the order lemma, we have $n \mid \varphi(p^k)$, so it suffices to prove that $\varphi(p^k) \mid n$. As $g^{p-1} = 1+ap$ with $p \nmid a$, we have $\mathrm{ord}_{p^k}(g^{p-1}) = p^{k-1}$ by the previous result. Since $(g^{p-1})^n = (g^n)^{p-1} \equiv 1 \bmod p^k$, the order lemma gives $p^{k-1} \mid n$. As g is a primitive root modulo p, we also have $(p-1) \mid n$. Since p^k and $p-1$ are coprime, we see that n is divisible by $p^{k-1}(p-1) = \varphi(p^k)$.

□

Example 1.7.11. As 2 is a primitive root modulo 3, and $2^2 \not\equiv 1 \bmod 9$, we see that 2 is a primitive root modulo 3^k for any $k \geqslant 2$.

We saw that $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is trivial for $k = 1$, and cyclic of order 2 for $k = 2$. What happens modulo 4 and 8?

Theorem 1.7.12. *Let $k \geqslant 3$ be an integer. Then*

$$\begin{aligned}(\mathbb{Z}/2^k\mathbb{Z})^\times &= \{(-1)^a 5^b : a \in \{0,1\}, b \in \{0,1,\ldots,2^{k-2}-1\}\} \bmod 2^k \\ &\simeq C_2 \times C_{2^{k-2}}.\end{aligned}$$

Example 1.7.13.

b	$5^b \bmod 16$	$-5^b \bmod 16$
0	1	15
1	5	11
2	9	7
3	13	3

Proof. We show by induction that

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} \bmod 2^k.$$

This holds for $k = 3$, so let's now assume it for a specific value of $k \geqslant 3$ and prove it with $k+1$ in place of k. Inserting the inductive hypothesis into the power-up lemma gives

$$5^{2^{k-2}} \equiv (1 + 2^{k-1})^2 \equiv 1 + 2^k \bmod 2^{k+1},$$

completing the induction. Now we also have

$$5^{2^{k-2}} \equiv 1 \bmod 2^k,$$

so $\mathrm{ord}_{2^k}(5) = 2^{k-2}$.

We need to show that the numbers $(-1)^a 5^b$ are incongruent modulo 2^k. Let $a, a', b, b' \in \mathbb{Z}$ with

$$0 \leqslant a \leqslant a' \leqslant 1, \qquad 0 \leqslant b \leqslant b' \leqslant 2^{k-2} - 1$$

and

$$(-1)^a 5^b \equiv (-1)^{a'} 5^{b'} \bmod 2^k.$$

Then

$$(-1)^a \equiv (-1)^{a'} \bmod 4,$$

so $a \equiv a' \bmod 2$, so $a = a'$. Now

$$5^{b'-b} \equiv 1 \bmod 2^k,$$

so $b \equiv b' \bmod 2^{k-2}$, whence $b = b'$. □

Using the algebraic Chinese remainder theorem to combine our structural results about the groups $(\mathbb{Z}/p^k\mathbb{Z})^\times$ for p prime and $k \in \mathbb{N}$, we reach a full classification of which moduli have primitive roots.

Theorem 1.7.14. *Let $m \geqslant 2$ be an integer. If $m = 2$, or $m = 4$, or $m = p^k$ with p an odd prime and $k \in \mathbb{N}$, or $m = 2p^k$ with p an odd prime and $k \in \mathbb{N}$, then there's a primitive root modulo m. Otherwise, there isn't.*

1.8 Quadratic residues

Given $m \in \mathbb{N}$, an integer a is a *quadratic residue* modulo m if there exists $x \in \mathbb{Z}$ such that $x^2 \equiv a \bmod m$. Otherwise, it's a *quadratic non-residue*.

Lemma 1.8.1 (Square roots lemma)**.** *Let p be an odd prime, and let $a \in \mathbb{Z}$ with $p \nmid a$. Then:*

(a) The number of $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $x^2 \equiv a \bmod p$ is either 2 or 0.

(b) There are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues in $(\mathbb{Z}/p\mathbb{Z})^\times$.

Proof. (a) If $x^2 \equiv a \bmod p$ then $(-x)^2 \equiv a \bmod p$, and $-x \not\equiv x \bmod p$ because p is odd and $p \nmid x$. Thus, it's impossible for there to be exactly one solution, and, by the general roots lemma, there can't be more than two solutions.

(b) By (a), there's a two-to-one function from $(\mathbb{Z}/p\mathbb{Z})^\times$ to its squares. The image of this function has size $(p-1)/2$.

□

For p an odd prime and $a \in \mathbb{Z}$, the *Legendre symbol* is given by

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

Example 1.8.2. Let's check out the case $p = 5$.

x	0	1	2	3	4
$\left(\frac{x}{5}\right)$	0	1	-1	-1	1

Remark 1.8.3. The Legendre symbol generalises to the Jacobi symbol, which in turn generalises to the Kronecker symbol. The Legendre symbol also generalises to the power residue symbols. We won't use any of these generalisations. If you do, then please handle them with care. Note in particular that if m is composite and $a \in \mathbb{Z}$ then $\left(\frac{a}{m}\right) = 1$ does **not** mean that a is a quadratic residue modulo m.

Theorem 1.8.4 (Euler's criterion)**.** *Let p be an odd prime, and let $a \in \mathbb{Z}$ with $p \nmid a$. Then*

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

Proof. By Wilson's theorem, we have $(p-1)! \equiv -1 \bmod p$, so it suffices to prove that

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

First suppose $\left(\frac{a}{p}\right) = 1$, and let $x \in \{1, 2, \ldots, p-1\}$ be an integer such that $x^2 \equiv a \bmod p$. Then

$$x(p-x) \equiv -x^2 \equiv -a \bmod p,$$

so

$$(p-1)! \equiv -a \prod_{\substack{j=1 \\ j \notin \{x, p-x\}}}^{p-1} j \bmod p.$$

We know from the squares roots lemma that the congruence $z^2 \equiv a \bmod p$ has precisely two solutions modulo p given by $z = x$ and $z = p - x$, so each j in the product can be paired with $y \neq j$ such that $jy \equiv a \bmod p$. There are $(p-3)/2$ such pairs, so

$$(p-1)! \equiv -aa^{(p-3)/2} \equiv -a^{(p-1)/2} \bmod p.$$

If a is a quadratic non-residue, then we get $(p-1)/2$ pairs and so

$$(p-1)! \equiv a^{(p-1)/2} \bmod p.$$

Either way, we have

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

completing the proof. □

Corollary 1.8.5. *Let p be an odd prime, and let $a, b \in \mathbb{Z}$. Then*

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

To compute any Legendre symbol $\left(\frac{a}{p}\right)$, it suffices to handle the special cases in which $a = -1$, $a = 2$, or a is an odd prime. We'll use *quadratic reciprocity* to deal with the case in which a is an odd prime. First, let's discuss the other cases. We already know about the case $a = -1$, from Euler's criterion.

Corollary 1.8.6 (First supplement to quadratic reciprocity)**.** *Let p be an odd prime. Then*

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

For the case $a = 2$, we'll use Gauss's lemma in number theory.

Lemma 1.8.7 (Gauss's lemma)**.** *Let p be an odd prime, and let $a \in \mathbb{Z}$ with $p \nmid a$. Denote by $\mu = \mu(a, p)$ the number elements of*

$$\left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}$$

that lie in

$$\left\{-1, -2, \ldots, \frac{1-p}{2}\right\} \bmod p.$$

Then

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

Proof. Let j and k be distinct elements of $\{1, 2, \ldots, \frac{p-1}{2}\}$. By Euclid's lemma and the observation that $1 \leqslant j + k \leqslant p - 1$, we have $p \nmid (ja \pm ka)$. We can reduce these elements ja modulo p so that they are non-zero integers in the range $[(1-p)/2, (p-1)/2]$, and their absolute values are then distinct. Thus, these absolute values are $1, 2, \ldots, (p-1)/2$, and μ of them come with a minus sign. Therefore

$$(-1)^{\mu} \prod_{j \leqslant \frac{p-1}{2}} j \equiv \prod_{j \leqslant \frac{p-1}{2}} (aj) \equiv a^{(p-1)/2} \prod_{j \leqslant \frac{p-1}{2}} j \bmod p.$$

Finally, as the product is invertible modulo p, we have

$$(-1)^{\mu} \equiv a^{(p-1)/2} \bmod p,$$

and Euler's criterion tells us that the right hand side is $\left(\frac{a}{p}\right) \bmod p$. □

Corollary 1.8.8 (Second supplement to quadratic reciprocity)**.** *Let p be an odd prime. Then*

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

Example 1.8.9. As $23 \equiv -1 \bmod 8$, we see that 2 is a quadratic residue modulo 23. Can you see this more explicitly?

Proof. Specialising $a = 2$ in Gauss's lemma gives

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

where μ counts elements of

$$\{2, 4, 6, \ldots, p-1\}$$

that lie in

$$\left\{\frac{p+1}{2}, \ldots, p-1\right\}.$$

These are given by $p - 1 - 2j$, where

$$0 \leqslant j \leqslant \frac{p-3}{4},$$

so

$$\mu = \left\lfloor \frac{p+1}{4} \right\rfloor.$$

If $p \equiv \pm 1 \bmod 8$ then μ is even, and otherwise it's odd. □

Lemma 1.8.10 (Odd variant of Gauss's lemma)**.** *Let p be an odd prime, and let $a \in \mathbb{Z}$ be odd with $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j \leqslant (p-1)/2} \lfloor ja/p \rfloor}.$$

Proof. Denote by J the set of positive integers $j \leqslant \frac{p-1}{2}$ such that ja lies in

$$\left\{-1, -2, \ldots, \frac{1-p}{2}\right\} \bmod p.$$

By Gauss's lemma, we have

$$\left(\frac{a}{p}\right) = (-1)^{\mu}, \qquad \mu = \#J.$$

Observe that if $j \leqslant \frac{p-1}{2}$ is a positive integer then

$$ja - p\left\lfloor \frac{ja}{p} \right\rfloor - p1_J(j)$$

lies between $\frac{1-p}{2}$ and $\frac{p-1}{2}$, and is congruent to ja modulo p.

We saw in the proof of Gauss's lemma that these numbers are, up to sign, the numbers $1, 2, \ldots, \frac{p-1}{2}$ in some order. Signs don't affect parity, so

$$\sum_{j \leqslant \frac{p-1}{2}} \left(ja - p\left\lfloor \frac{ja}{p} \right\rfloor - p1_J(j) \right) \equiv \sum_{j \leqslant \frac{p-1}{2}} j \equiv \frac{1}{2}\,\frac{p-1}{2}\,\frac{p+1}{2} \equiv \frac{p^2-1}{8} \bmod 2.$$

On the other hand, direct computation yields

$$\begin{aligned} \sum_{j \leqslant \frac{p-1}{2}} \left(ja - p\left\lfloor \frac{ja}{p} \right\rfloor - p1_J(j) \right) &= a \sum_{j \leqslant \frac{p-1}{2}} j - p \sum_{j \leqslant \frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - p\mu \\ &= \frac{a(p^2-1)}{8} - p \sum_{j \leqslant \frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - p\mu. \end{aligned}$$

As a, p are odd, and odd squares are 1 mod 8, we obtain

$$p \sum_{j \leqslant \frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor \equiv p\mu + \frac{(a-1)(p^2-1)}{8} \equiv p\mu \bmod 2,$$

whence

$$\mu \equiv \sum_{j \leqslant \frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor \bmod 2.$$

Therefore

$$\left(\frac{a}{p}\right) = (-1)^{\mu} = (-1)^{\sum_{j \leqslant \frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor}.$$

□

We come to our main result about quadratic residues.

Theorem 1.8.11 (Law of quadratic reciprocity, Gauss, 1796)**.** *Let $p \neq q$ be odd primes. Then*

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

In other words, if p and q are distinct odd primes, then

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

Proof. Let

$$N = \frac{(p-1)(q-1)}{4}$$

be the number of pairs $(x, y) \in \mathbb{N}^2$ such that $x \leqslant p/2$ and $y \leqslant q/2$. Then $N = N_1 + N_2$, where N_1 counts those pairs for which $y < qx/p$ and N_2 counts those pairs for which $y > qx/p$. We have

$$N_1 = \sum_{x \leqslant \frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor, \qquad N_2 = \sum_{y \leqslant \frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor,$$

so

$$\sum_{x \leqslant \frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y \leqslant \frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor = \frac{(p-1)(q-1)}{4}.$$

The odd variant of Gauss's lemma now yields

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

whence

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

□

We're now equipped to compute general Legendre symbols.

Example 1.8.12. We compute that

$$\begin{aligned} \left(\frac{103}{83}\right) &= \left(\frac{20}{83}\right) = \left(\frac{5}{83}\right) \\ &= \left(\frac{83}{5}\right) = \left(\frac{3}{5}\right) = -1, \end{aligned}$$

so 103 is a quadratic non-residue modulo 83.

What about higher powers?

Lemma 1.8.13. *Let $m \in \mathbb{N}$ with $(\mathbb{Z}/m\mathbb{Z})^\times$ cyclic, let $a \in \mathbb{Z}$ be coprime to m, and let $n \in \mathbb{N}$. Then a is an n^{th} power residue if and only if $a^{\varphi(m)/(n,\varphi(m))} \equiv 1 \bmod m$.*

Proof. We want to solve

$$x^n \equiv a \bmod m.$$

Let g be a primitive root modulo m, and let $b, y \in \mathbb{N}$ with

$$a \equiv g^b \bmod m, \qquad x \equiv g^y \bmod m.$$

Our congruence becomes

$$g^{ny} \equiv g^b \bmod m,$$

which is equivalent to $ny \equiv b \bmod \varphi(m)$ by the order lemma. This has a solution if and only if $d \mid b$, where

$$d = (n, \varphi(m)).$$

The upshot is that a is an n^{th} power residue if and only if $d \mid b$.

If $d \mid b$ then

$$a^{\varphi(m)/d} \equiv g^{b\varphi(m)/d} \equiv 1 \bmod m,$$

by Euler's theorem. Conversely, if $a^{\varphi(m)/d} \equiv 1 \bmod m$, then

$$g^{b\varphi(m)/d} \equiv 1 \bmod m,$$

so $\varphi(m)$ divides $b\varphi(m)/d$, and finally $d \mid b$. □

2 Diophantine equations

These are equations where we consider integer solutions. We'll be considering equations defined by the vanishing of a polynomial. Key data include its degree, the number of variables, and whether the polynomial is homogeneous. Our polynomials will be fairly tame in the sense that they won't contain 'cross terms' such as xy. Nonetheless, we'll see rich theories on linear combinations of squares and higher powers, which neatly demonstrate the interaction between addition and multiplication.

2.1 The geometry of numbers

This is about counting lattice points in Euclidean regions. There's a Lipschitz principle that if the region is nice then the number of lattice points should be roughly the volume, after a suitable normalisation if appropriate.

Example 2.1.1 (Gauss circle problem, non-examinable)**.** For $R \geqslant 1$, write

$$N(R) = \#\{(x, y) \in \mathbb{Z}^2 : x^2 + y^2 \leqslant R^2\}.$$

This is the number of integer pairs within a circle of radius R centred at the origin. One can use the geometry to estimate $N(R)$ by the area πR^2, with an error of at most a constant times the circumference $2\pi R$. Gauss argued in this way to show that the error

$$E(R) = N(R) - \pi R^2$$

satisfies

$$|E(R)| \leqslant 2\sqrt{2}\pi R.$$

The Gauss circle problem is to bound this error asymptotically. The record is held by Huxley, who showed that if $\theta > 131/208 \approx 0.63$ then there exists $C = C(\theta)$ such that

$$E(R) \leqslant CR^\theta$$

for all R. The optimal exponent is believed to be $1/2$.

Our study of quadratic diophantine equations will require a key result about lattice points in symmetric, convex bodies, called *Minkowski's theorem*. This won't be as precise as counting lattice points accurately. Under suitable

conditions, it will tell us that there's at least one lattice point, once the volume of the region exceeds a large multiple of the covolume of the lattice.

Let $n \in \mathbb{N}$. A (full) *lattice* in $\mathbb{R}^n$ is

$$\Lambda = \{a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n : a_1, \ldots, a_n \in \mathbb{Z}\},$$

where $\mathbf{u}_1, \ldots, \mathbf{u}_n \in \mathbb{R}^n$ are linearly independent vectors.

Example 2.1.2. The standard Euclidean basis generates the lattice $\mathbb{Z}^n$.

We say that $\mathbf{u}_1, \ldots, \mathbf{u}_n$ form a *basis* for the lattice Λ. They form a square matrix whose absolute determinant

$$\det(\Lambda) = |\det(\mathbf{u}_1, \ldots, \mathbf{u}_n)|$$

is called the *determinant* of the lattice.

Lemma 2.1.3. *The determinant of a lattice is well defined.*

Proof. Let $\mathbf{u}_1, \ldots, \mathbf{u}_n$ and $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be bases for a lattice Λ in $\mathbb{R}^n$. Then there are $n \times n$ integer matrices $A = (a_{i,j})$ and $B = (b_{j,k})$ such that

$$\mathbf{u}_i = \sum_j a_{i,j}\mathbf{v}_j \quad (1 \leqslant i \leqslant n), \qquad \mathbf{v}_j = \sum_k b_{j,k}\mathbf{u}_k \quad (1 \leqslant j \leqslant n).$$

Thus $U = AV$ and $V = BU$, where

$$U = (\mathbf{u}_1, \ldots, \mathbf{u}_n), \qquad V = (\mathbf{v}_1, \ldots, \mathbf{v}_n),$$

and in particular

$$B = VU^{-1} = (UV^{-1})^{-1} = A^{-1}.$$

Now $\det(A)\det(B) = 1$, so $\det(A) = \pm 1$. Finally, as determinants respect products, we have

$$|\det(U)| = |\det(A)| \cdot |\det(V)| = |\det(V)|.$$

□

The determinant of Λ is, equivalently, the volume of the *fundamental domain*

$$D_0 = \left\{ \sum_i x_i\mathbf{u}_i : 0 \leqslant x_i < 1 \right\}.$$

Euclidean space $\mathbb{R}^n$ is tiled by the lattice translates of D_0. As volume is translation-invariant, we have

$$\det(\Lambda) = \mathrm{vol}(D)$$

for any such translate D.

Example 2.1.4. The lattice $\mathbb{Z}^n$ has determinant 1. The fundamental domain, with respect to the standard Euclidean basis, is a unit hypercube.

A set $S \subseteq \mathbb{R}^n$ is *symmetric* for $-\mathbf{x} \in S$ for all $\mathbf{x} \in S$. It is *convex* if, for any $\mathbf{x}, \mathbf{y} \in S$, the line segment

$$\{t\mathbf{x} + (1-t)\mathbf{y} : 0 \leqslant t \leqslant 1\}$$

between them is contained in S.

Theorem 2.1.5 (Minkowski's theorem, 1891)**.** *Let Λ be a lattice in $\mathbb{R}^n$, and let $S \subseteq \mathbb{R}^n$ be a symmetric, convex set whose volume exceeds $2^n\det(\Lambda)$. Then S contains a non-zero lattice point.*

We introduce some notation for its proof. For $t > 0$, we write

$$tS = \{t\mathbf{x} : \mathbf{x} \in S\}.$$

For $X, Y \subseteq \mathbb{R}^n$, we write

$$X + Y = \{\mathbf{x} + \mathbf{y} : \mathbf{x} \in X,\ \mathbf{y} \in Y\}.$$

Proof. By intersecting with a large ball, we may assume that S has finite volume. It suffices to prove that there are two distinct point $\mathbf{x}, \mathbf{x}' \in R := \frac{1}{2}S$ whose difference lies in Λ. Indeed, if this is the case then symmetry yields

$$2\mathbf{x}, -2\mathbf{x}' \in S,$$

and then by convexity S also contains their midpoint $\mathbf{x} - \mathbf{x}'$.

Summing over lattice translates of D_0, where $\lambda_D + D = D_0$, observe that

$$\begin{aligned}\sum_D \mathrm{vol}(\lambda_D + (R \cap D)) = \sum_D \mathrm{vol}(R \cap D) &= \mathrm{vol}(R) = 2^{-n}\mathrm{vol}(S) \\ &> \det(\Lambda) = \mathrm{vol}(D_0).\end{aligned}$$

Each $\lambda_D + (R \cap D)$ is a subset of D_0, so these sets cannot be disjoint. Thus, there exist $\mathbf{x}, \mathbf{x}' \in R$ and distinct $\lambda, \lambda' \in \Lambda$ such that

$$\lambda + \mathbf{x} = \lambda' + \mathbf{x}'.$$

Finally, we have $\mathbf{x} - \mathbf{x}' = \lambda' - \lambda \in \Lambda$. □

We'll see Minkowski's theorem in action soon enough. If the set is compact (closed and bounded), then the inequality doesn't need to be strict. We deduce this from Minkowski's theorem using Cantor's intersection theorem, which asserts that if

$$C_1 \supset C_2 \supset \dots$$

are non-empty, compact subsets of $\mathbb{R}^n$ then their intersection is non-empty.

Corollary 2.1.6 (Strong form of Minkowski's theorem)**.** *Let Λ be a lattice in $\mathbb{R}^n$, and let $S \subset \mathbb{R}^n$ be a compact, symmetric, convex set whose volume is greater than or equal to $2^n \det(\Lambda)$. Then S contains a non-zero lattice point.*

Proof. Given $k \in \mathbb{N}$, the set

$$S_k = \left(1 + \frac{1}{k}\right) S$$

is symmetric and convex, and has volume exceeding $2^n \det(\Lambda)$, so it must contain a non-zero lattice point. By Cantor's intersection theorem, the intersection of the compact sets $S_k \cap (\Lambda \setminus \{\mathbf{0}\})$ is non-empty. Finally, if $\mathbf{x}$ lies in this intersection then

$$\left(1 - \frac{1}{k+1}\right) \mathbf{x} \in S \qquad (k \in \mathbb{N})$$

so, as S is closed, the accumulation point $\mathbf{x}$ must also lie in S. □

We'll use the strong form of Minkowski's theorem later, but not before we've used the standard version a couple of times!

2.2 Sums of squares

Which numbers can be written as a sum of two squares? Clearly not numbers that are 3 mod 4. The following result is often attributed to Fermat, though it would seem that its proof was only completed by Euler in 1760.

Theorem 2.2.1. *Let $p \equiv 1 \bmod 4$ be prime. Then p is a sum of two squares.*

Proof. We know that -1 is a square modulo p, so let m be an integer such that

$$m^2 \equiv -1 \bmod p.$$

The lattice Λ spanned by $(1, m)$ and $(0, p)$ has determinant p. The symmetric, convex body

$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 2p\}$$

has area $2\pi p > 4p = 2^2 \det(\Lambda)$, so it contains

$$(x, y) = a(1, m) + b(0, p) = (a, am + bp)$$

for some $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. As

$$x^2 + y^2 \equiv a^2 + a^2 m^2 = a^2(1 + m^2) \equiv 0 \bmod p$$

and $0 < x^2 + y^2 < 2p$, we must have $x^2 + y^2 = p$. □

The set of sums of two squares is closed under multiplication, which will enable us to strengthen the previous result considerably.

Lemma 2.2.2. *If $a, b \in \mathbb{N}$ are sums of two squares, then so too is ab.*

Proof. Let $x, y, z, w \in \mathbb{Z}$ with $a = x^2 + y^2$ and $b = z^2 + w^2$. Then

$$(xz+yw)^2+(xw-yz)^2 = x^2z^2+y^2w^2+x^2w^2+y^2z^2 = (x^2+y^2)(z^2+w^2) = ab.$$

□

In order to fully classify numbers that are a sum of two squares, we also require some information in the opposite direction.

Lemma 2.2.3. *Let $x, y \in \mathbb{Z}$, and suppose a prime $p \equiv 3 \bmod 4$ divides $x^2 + y^2$. Then $p \mid x$ and $p \mid y$.*

Proof. If $p \nmid x$ then $(yx^{-1})^2 \equiv -1 \bmod p$, contradicting that $\left(\frac{-1}{p}\right) = -1$. Thus $p \mid x$, and by symmetry $p \mid y$. □

Corollary 2.2.4. *If $n \in \mathbb{N}$ is a sum of two squares and $p \equiv 3 \bmod 4$ is a prime divisor of n, then $p^2 \mid n$, and n/p^2 is a sum of two squares.*

Finally, we require a concept that's generally useful in number theory. A prime power p^k *exactly divides* an integer n if

$$p^k \mid n, \qquad p^{k+1} \nmid n,$$

and we write $p^k \| n$ if this occurs. If $n \neq 0$, then there is a unique such value of k, which we denote by $\nu_p(n)$ and call the *p-adic order* of n. We define $\nu_p(0) = \infty$.

Theorem 2.2.5 (Two-square theorem)**.** *A positive integer n can be expressed as a sum of two squares if and only if, for any prime $p \equiv 3 \bmod 4$, we have $\nu_p(n) \equiv 0 \bmod 2$.*

Proof. Suppose $\nu_p(n)$ is even for each prime $p \equiv 3 \bmod 4$. Then $n = ab^2$ for some $a, b \in \mathbb{N}$, where a has no prime divisors that are 3 mod 4. As 2 is a sum of two squares, and any $p \equiv 1 \bmod 4$ is a sum of two squares, multiplicative closure implies that a is a sum of two squares, say $a = x^2 + y^2$. Now $ab^2 = (xb)^2 + (yb)^2$.

Conversely, if n is a sum of two squares then, for any prime $p \equiv 3 \bmod 4$ dividing n, we have $p^2 \mid n$ and that n/p^2 is a sum of two squares. Repeating this argument, we conclude that $\nu_p(n)$ is even for each prime $p \equiv 3 \bmod 4$. □

There's a similar criterion for sums of three squares that we shan't prove. Recall that we saw the congruence obstruction earlier.

Theorem 2.2.6 (Legendre's three-square theorem)**.** *A positive integer is a sum of three squares if and only if it's not of the form*

$$4^a(8b + 7),$$

where $a, b \in \mathbb{Z}_{\geqslant 0}$.

Example 2.2.7. As

$$2028 = 4 \times 507, \qquad 507 \equiv 7 \bmod 8,$$

we can't write 2028 as a sum of three squares.

We'll show that any positive integer is a sum of four squares. Be careful, as zero needs to count as a square here! Show as an exercise that if k is odd then 2^k is not a sum of exactly four **positive** squares.

As with sums of two squares, the set of sums of four squares is closed under multiplication.

Lemma 2.2.8. *If $a, b \in \mathbb{N}$ are sums of four squares, then so too is ab.*

Proof. You can check the identity

$$\begin{aligned}&(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_2^3+y_4^2)\\&=(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2\\&\qquad+(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2\end{aligned}$$

using your favourite computer algebra software. □

Theorem 2.2.9 (Lagrange's four-square theorem)**.** *Any positive integer is a sum of four squares.*

Example 2.2.10. Let's write 2024 as a sum of four squares. We have

$$2024-44^2=88=4(9+9+4),$$

so

$$2024=44^2+6^2+6^2+4^2.$$

Now try writing it as a sum of three squares.

Proof. By multiplicative closure and the fact that $2=1^2+1^2+0^2+0^2$, it suffices to show that any odd prime is a sum of four squares. Let p be an odd prime. We'll find $x,y,z,w\in\mathbb{Z}$ such that $x^2+y^2+z^2+w^2$ is divisible by p and lies in the interval $(0,2p)$, which will complete the proof.

The sets

$$\{a^2:a\in\mathbb{Z}/p\mathbb{Z}\},\qquad\{-b^2-1:b\in\mathbb{Z}/p\mathbb{Z}\}$$

each have cardinality $(p+1)/2$, so they must intersect. Hence

$$a^2+b^2\equiv-1 \bmod p,$$

for some $a,b\in\mathbb{Z}$. If (x,y,z,w) lie in

$$\Lambda=\{(x,y,z,w)\in\mathbb{Z}^4:z\equiv ax+by \bmod p,\quad w\equiv ay-bx \bmod p\},$$

then

$$\begin{aligned}x^2+y^2+z^2+w^2&\equiv x^2+y^2+(ax+by)^2+(bx-ay)^2\\&\equiv x^2+y^2+(a^2+b^2)x^2+(a^2+b^2)y^2\\&\equiv(a^2+b^2+1)(x^2+y^2)\equiv0 \bmod p.\end{aligned}$$

Observe that

$$\begin{pmatrix} 1 \\ 0 \\ a \\ -b \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \\ b \\ a \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 0 \\ p \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 0 \\ 0 \\ p \end{pmatrix}$$

form a basis for the lattice Λ, and that $\det(\Lambda) = p^2$. The symmetric, convex body

$$\{(x, y, z, w) \in \mathbb{R}^4 : x^2 + y^2 + z^2 + w^2 < 2p\}$$

has volume

$$\frac{\pi^2}{2}(\sqrt{2p})^4 = 2\pi^2 p^2 > 2^4 \det(\Lambda),$$

so it contains a non-zero element of Λ. □

2.3 Gaussian primes

The ring of *Gaussian integers* is

$$\mathbb{Z}[i] = \{x + yi : x, y \in \mathbb{Z}\}.$$

Given $\alpha, \beta \in \mathbb{Z}[i]$, we say that α *divides* β, and write $\alpha \mid \beta$, if there exists $\gamma \in \mathbb{Z}[i]$ such that $\alpha\gamma = \beta$. For $x, y \in \mathbb{Z}$, the *norm* of $\alpha = x + yi$ is

$$N(\alpha) = |\alpha|^2 = x^2 + y^2 \in \mathbb{Z}_{\geqslant 0}.$$

Thus, sums of two squares are precisely norms of Gaussian integers. It's convenient for us to write $N(\alpha) = |\alpha|^2$ for $\alpha \in \mathbb{C}$.

Lemma 2.3.1. *If $\alpha, \beta \in \mathbb{C}$ then $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Proof. We have

$$N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2 = N(\alpha)N(\beta).$$

□

A *unit* in a ring is an invertible element.

Lemma 2.3.2. *The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.*

Proof. Observe that $\pm 1, \pm i$ are precisely the elements of norm one. Let $\alpha \in \mathbb{Z}[i]$.

First suppose $N(\alpha) = 1$. Then $\alpha\bar{\alpha} = 1$, so α is a unit.

Conversely, suppose α is a unit. Then, for some $\beta \in \mathbb{Z}[i]$, we have $\alpha\beta = 1$. Hence

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1,$$

so $N(\alpha) = 1$. □

Lemma 2.3.3 (Division algorithm in the Gaussian integers)**.** *Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. Then there exist $\gamma, \delta \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma + \delta$ and $N(\delta) < N(\beta)$.*

Note that we have not claimed uniqueness.

Proof. Let $\gamma \in \mathbb{Z}[i]$ with $|\alpha/\beta - \gamma|$ minimal, so that

$$N(\alpha/\beta - \gamma) \leqslant \frac{1}{2} < 1.$$

Then, with $\delta = \alpha - \beta\gamma$, we have

$$N(\delta) = N(\alpha/\beta - \gamma)N(\beta) < N(\beta).$$

□

Example 2.3.4. Let's divide $\alpha = 4 + 5i$ by $\beta = 3$ with remainder in the Gaussian integers. We have

$$\frac{4 + 5i}{3} = \frac{4}{3} + \frac{5}{3}i,$$

so we can take $\gamma = 1 + 2i$ as our quotient and $\delta = 1 - i$ as our remainder:

$$4 + 5i = (1 + 2i)3 + (1 - i).$$

We check that $N(1 - i) = 2 < 9 = N(3)$. Can you identify the other solutions?

Given $\alpha, \beta \in \mathbb{Z}[i]$, not both zero, a *greatest common divisor* (GCD) of a and b is a common divisor of maximal norm. As we have the division algorithm, the extended Euclidean algorithm carries through in $\mathbb{Z}[i]$, expressing any greatest common divisor as a linear combination of the two Gaussian integers.

Lemma 2.3.5 (Bézout's lemma in the Gaussian integers)**.** *Let δ be a GCD of $\alpha, \beta \in \mathbb{Z}[i]$. Then there exist $\kappa, \lambda \in \mathbb{Z}[i]$ such that*

$$\kappa\alpha + \lambda\beta = \delta.$$

Example 2.3.6. Let's compute a GCD of $4 + 5i$ and 3, in $\mathbb{Z}[i]$, and write it as a linear combination of $4 + 5i$ and 3. We have

$$\begin{aligned} 4 + 5i &= (1 + 2i)3 + (1 - i) \\ 3 &= (1 + i)(1 - i) + 1 \\ 1 - i &= (1 - i)1, \end{aligned}$$

so 1 is a GCD and

$$\begin{aligned} 1 &= 3 - (1 + i)(1 - i) \\ &= 3 - (1 + i)(4 + 5i - (1 + 2i)3) \\ &= (3i)3 - (1 + i)(4 + 5i). \end{aligned}$$

A *Gaussian prime* is a non-zero, non-unit Gaussian integer π such that if $\alpha, \beta \in \mathbb{Z}[i]$ and $\pi \mid \alpha\beta$ then $\pi \mid \alpha$ or $\pi \mid \beta$. This is motivated by Euclid's lemma, and is equivalent to the following notion. A Gaussian integer is *irreducible* if it is non-zero, not a unit, and cannot be expressed as a product of two non-units.

Lemma 2.3.7. *Let π be a non-zero, non-unit Gaussian integer. Then π is a Gaussian prime if and only if it's irreducible.*

Proof. First suppose π is a Gaussian prime, and that $\pi = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$. Then $\pi \mid \alpha$ or $\pi \mid \beta$, so we may assume without loss that $\pi \mid \alpha$. Now $\alpha = \pi\gamma$ for some $\gamma \in \mathbb{Z}[i]$, so

$$\pi = \alpha\beta = \pi\gamma\beta.$$

Therefore $\gamma\beta = 1$, and in particular β is a unit. We conclude that π is irreducible.

Now suppose instead that π is irreducible, and that $\pi \mid \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$. Let δ be a GCD of π, α. By Bézout's lemma, there exist $\kappa, \lambda \in \mathbb{Z}[i]$ such that

$$\kappa\pi + \lambda\alpha = \delta.$$

As π is irreducible, we must have that δ is a unit or a unit multiple of π. If δ is a unit then, as

$$\delta\beta = \kappa\pi\beta + \lambda\alpha\beta$$

is divisible by π, we must have $\pi \mid \beta$. If δ is a unit multiple of π, then $\pi \mid \alpha$. In each case, we have $\pi \mid \alpha$ or $\pi \mid \beta$, so π is a Gaussian prime. □

Lemma 2.3.8. *If π is a Gaussian prime then so is any unit multiple of π, and so is $\bar{\pi}$.*

Proof. Exercise. □

Lemma 2.3.9. *Let $\pi \in \mathbb{Z}[i]$ with $N(\pi)$ prime. Then π is a Gaussian prime.*

Proof. Suppose $\pi = \alpha\beta$ with $\alpha, \beta \in \mathbb{Z}[i]$. Then

$$N(\alpha)N(\beta) = N(\pi)$$

is prime, so $N(\alpha) = 1$ or $N(\beta) = 1$, so α is a unit or β is a unit. □

Example 2.3.10. As $N(1+i) = 2$ is prime, we see that $1+i$ is a Gaussian prime.

Example 2.3.11. In spite of not having prime norm, the integer 3 is a Gaussian prime. Indeed, suppose $3 = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$. Then

$$N(\alpha)N(\beta) = 9$$

and, as 3 is not a sum of two squares, we must have $N(\alpha) = 1$ or $N(\beta) = 1$, so α is a unit or β is a unit.

Adapting this example gives the following.

Lemma 2.3.12. *If $p \equiv 3 \bmod 4$ is prime then p is a Gaussian prime.*

Theorem 2.3.13 (Unique factorisation)**.** *Any non-zero, non-unit Gaussian integer is a product of Gaussian primes. This expression is unique, up to re-ordering and multiplication by units.*

Proof. Let $\alpha \in \mathbb{Z}[i]$. We start with existence. Our inductive base is the case $N(\alpha) = 2$. As $N(\alpha)$ is prime, we must have that α is a Gaussian prime.

Next, suppose that any Gaussian integer of norm in $[2, N(\alpha) - 1]$ is a product of Gaussian primes. If α is not a Gaussian prime, then we have

$$\alpha = \beta\gamma$$

for some $\beta, \gamma \in \mathbb{Z}[i]$ whose norms are in $[2, N(\alpha) - 1]$. By our inductive hypothesis, we can write β and γ as a product of Gaussian primes, and hence we can also express α as a product of Gaussian primes.

We come to uniqueness. Any factorisation of α into Gaussian primes can be written as

$$\alpha = \mu_0\pi_1 \cdot \pi_k,$$

where μ_0 is a unit and $\pi_1, \dots \pi_k$ are Gaussian primes, normalised to have positive real part and non-negative imaginary part. If two such expressions are equal, then we can divide out by common factors, giving

$$\pi_1 \cdots \pi_s = \mu\psi_1 \cdots \psi_t,$$

where $\{\pi_i\}$ and $\{\psi_j\}$ are disjoint and μ is a unit, and $s \geqslant 1$. Now π_1 divides some ψ_j, and therefore equals ψ_j by normalisation, contradicting disjointness. □

We'll see an example of this shortly. First, we need to determine what the Gaussian primes are!

Theorem 2.3.14 (Classification of Gaussian primes)**.** *The following is a complete list of Gaussian primes.*

- *Prime $p \equiv 3 \bmod 4$ times a unit.*
- *$\alpha \in \mathbb{Z}[i]$ such that $N(\alpha)$ is prime.*

Proof. We've seen that these are Gaussian primes. Now suppose $\alpha = x + yi$ is a Gaussian prime, where $x, y \in \mathbb{Z}$, and let p be a prime divisor of $N(\alpha) = x^2 + y^2$.

First suppose $p = 2$. Then $x \equiv y \bmod 2$ and

$$\alpha = (1 + i)\left(\frac{x + y}{2} + \frac{y - x}{2}i\right).$$

Consequently, the second factor is a unit, and $N(\alpha) = 2$ is prime.

Next, suppose instead that $p \equiv 3 \bmod 4$. As p divides $x^2 + y^2$, Lemma 2.2.3 gives $p \mid x$ and $p \mid y$, so $p \mid \alpha$. Thus α is a unit multiple of p.

Finally, suppose instead that $p \equiv 1 \bmod 4$, and write $p = a^2 + b^2$ with $a, b \in \mathbb{N}$. It remains to show that α is divisible by $\pi := a+bi$ or $\bar{\pi}$ (whereupon $N(\alpha) = p$ is prime). We compute that

$$\frac{\alpha}{\pi} = \frac{\bar{\pi}\alpha}{N(\pi)} = \frac{(a-bi)(x+yi)}{a^2+b^2} = \frac{ax+by}{p} + \frac{ay-bx}{p}i$$

and

$$\frac{\alpha}{i\bar{\pi}} = \frac{-\pi i\alpha}{N(\pi)} = \frac{-i(a+bi)(x+yi)}{a^2+b^2} = \frac{(b-ai)(x+yi)}{p} = \frac{bx+ay}{p} + \frac{by-ax}{p}i.$$

Observe that

$$(by+ax)(by-ax) = b^2y^2 - a^2x^2 = (a^2+b^2)y^2 - a^2(x^2+y^2)$$

is divisible by p, as is

$$(ay-bx)(ay+bx) = a^2y^2 - b^2x^2 = (a^2+b^2)y^2 - b^2(x^2+y^2).$$

We now distinguish four cases.

Case: p divides $by+ax$ and $ay-bx$. Then $\pi \mid \alpha$.
Case: p divides $by-ax$ and $ay+bx$. Then $\bar{\pi} \mid \alpha$.
Case: p divides $by+ax$ and $ay+bx$. Then p divides

$$y(ax+by) - x(ay+bx) = b(y^2-x^2)$$

so, as p is too large to divide b, it must divide $y^2 - x^2$. Since p also divides $y^2 + x^2$, we see that $p \mid 2x^2$ and $p \mid 2y^2$. Now p divides x and y, and so $\pi \mid \alpha$.
Case: p divides $by-ax$ and $ay-bx$. Then p divides

$$y(by-ax) + x(ay-bx) = b(y^2-x^2),$$

so again $\pi \mid \alpha$. □

From the proof above, we also learn a bit more about factorisation in $\mathbb{Z}[i]$.

Lemma 2.3.15. *Let $\alpha \in \mathbb{Z}[i]$, and let p be a prime divisor of $N(\alpha)$. Then:*

(a) If $p = 2$ then $1 + i$ divides α.

(b) If $p \equiv 3 \bmod 4$ then $p \mid \alpha$.

(c) If $p = x^2 + y^2$ with $x, y \in \mathbb{N}$ then $x + yi$ or $x - yi$ divides α.

Example 2.3.16. Let's factorise $39 - 48i$ into Gaussian primes. Note that

$$39 - 48i = 3(13 - 16i),$$

and that 3 is a Gaussian prime. We have

$$N(13 - 16i) = 169 + 256 = 425 = 5^2 \times 17,$$

so $13 - 16i$ is divisible by $2 + i$ or $2 - i$. We compute that

$$\frac{13 - 16i}{2 + i} = \frac{(2 - i)(13 - 16i)}{5} = 2 - 9i,$$

which has norm 5×17. Moreover

$$\frac{2 - 9i}{2 + i} = \frac{(2 - i)(2 - 9i)}{5} = -1 - 4i.$$

Therefore

$$39 - 48i = 3(2 + i)^2(-1 - 4i),$$

and the factors $2 + i$, $-1 - 4i$ are Gaussian primes because their norms are prime.

2.4 Pythagorean triples

A *Pythagorean triple* is a solution $(x, y, z) \in \mathbb{N}^3$ to $x^2 + y^2 = z^2$. These are triples of positive integers that can be the side lengths of a right triangle.

Example 2.4.1. The simplest Pythagorean triple is $(3, 4, 5)$.

A Pythagorean triple (x, y, z) is *primitive* if $\gcd(x, y, z) = 1$. To motivate this definition, note that if (x, y, z) is a Pythagorean triple then so too is (dx, dy, dz) for any $d \in \mathbb{N}$. Note also that primitivity of (x, y, z) is equivalent to the coordinates being pairwise coprime, for if a prime divides two of the coordinates then it must divide the other. If (x, y, z) is a primitive Pythagorean triple, then we may assume that y is even, since $\bmod 4$ considerations prevent x and y from both being odd.

Theorem 2.4.2 (Parametrisation of Pythagorean triples, Diophantus, circa 250AD)**.** *A triple $(x, y, z) \in \mathbb{N}^3$ is a primitive Pythagorean triple, with y even, if and only if*

$$x = u^2 - v^2, \qquad y = 2uv, \qquad z = u^2 + v^2$$

for some coprime $u, v \in \mathbb{N}$, not both odd, such that $u > v$.

Proof. If x, y, z are of the given form then

$$z^2 - x^2 = 4u^2v^2 = y^2.$$

If, further, a prime p divides x and z, then $p \mid z \pm x$, so

$$p \mid (2u^2, 2v^2) = 2(u, v)^2 = 2.$$

This can't happen, since u and v have different parity. Thus the triple is primitive, and we've demonstrated the 'if' part.

For the 'only if' part, let (x, y, z) be a primitive Pythagorean triple, with y even. Then x and z are both odd, leading us to the factorisation

$$y^2 = 4ab, \qquad a = \frac{z + x}{2}, \qquad b = \frac{z - x}{2}.$$

Observe that if $d \in \mathbb{N}$ divides a and b then $d \mid a + b = z$ and $d \mid a - b = x$, so $d = 1$. Therefore a and b are coprime, and their product is a square, so a and b must be squares. Setting $u = \sqrt{a}$ and $v = \sqrt{b}$, it remains to show that a and b are not both odd. Assume for a contradiction that $a \equiv b \equiv 1 \bmod 2$. Then $z \pm x \equiv 2 \bmod 4$, so $2z \equiv 0 \bmod 4$, which is impossible as z is odd. □

2.5 Ternary quadratic equations

Here we consider equations of the form

$$ax^2 + by^2 = cz^2,$$

where $a, b, c \in \mathbb{N}$ are given. We look for non-trivial integer solutions, the trivial solution being $(0, 0, 0)$. We've seen in an exercise that if $(a, b, c) = (1, 1, 3)$ then there are no solutions. On the other hand, there are infinitely many solutions if $(a, b, c) = (1, 1, 1)$.

Theorem 2.5.1. *Let $a, b, c \in \mathbb{N}$ be squarefree and pairwise coprime. Then the equation*

$$ax^2 + by^2 = cz^2$$

has a non-trivial integer solution if and only if:

- *bc is a quadratic residue modulo a,*
- *ac is a quadratic residue modulo b, and*
- *$-ab$ is a quadratic residue modulo c.*

Proof. First suppose that (x, y, z) is a non-trivial solution to the equation. We may assume that the coordinates are pairwise coprime. Indeed, any prime divisor of two of them would divide the third, by the squarefree condition, and if p divides x, y, z then $(x/p, y/p, z/p)$ also solves the equation.

Multiplying by c yields

$$acx^2 + bcy^2 = (cz)^2,$$

so

$$bcy^2 \equiv (cz)^2 \bmod a.$$

Moreover, we have $(a, y) = 1$. Indeed, assume for a contradiction that $p \mid a$ and $p \mid y$. Then $p \mid cz^2$. Also $p \nmid c$, since $p \mid a$ and $(a, c) = 1$. Therefore $p \mid z$, contradicting the coprimality of y and z. This confirms that $(a, y) = 1$.

Now

$$bc \equiv (y^{-1}cz)^2 \bmod a.$$

Similarly, one can show that ac is a square modulo b and $-ab$ is a square modulo c.

For the converse, we apply the strong form of Minkowski's theorem. Let $r, s, t \in \mathbb{Z}$ with

$$r^2 \equiv bc \bmod a, \qquad s^2 \equiv ac \bmod b, \qquad t^2 \equiv -ab \bmod c.$$

Suppose (x, y, z) lies in the set

$$\Lambda = \{(x, y, z) \in \mathbb{Z}^3 : by \equiv rz \bmod a, \quad cz \equiv sx \bmod b, \quad ax \equiv ty \bmod c\}.$$

Then

$$bry \equiv r^2 z \equiv bcz \bmod a,$$

so as $(a, b) = 1$ we have $ry \equiv cz \bmod a$, and hence

$$ax^2 + by^2 - cz^2 \equiv by^2 - cz^2 \equiv rzy - cz^2 \equiv z(ry - cz) \equiv 0 \bmod a.$$

Similar arguments reveal that $ax^2 + by^2 - cz^2$ is divisible by b and c. As a, b, c are pairwise coprime, we thus have

$$ax^2 + by^2 - cz^2 \equiv 0 \bmod abc.$$

The congruences defining Λ can be rewritten as

$$y \equiv t_c^{-1} ax \bmod c, \qquad z \equiv c_b^{-1} sx \bmod b, \qquad z \equiv r_a^{-1} by \bmod a,$$

where t_c^{-1} denotes the inverse of t modulo c and so on. By the Chinese remainder theorem, we can write these congruences as

$$y \equiv \eta x \bmod c, \qquad z \equiv \tau x + \rho y \bmod ab,$$

for some $\eta, \tau, \rho \in \mathbb{Z}$. Now

$$y = \eta x + cu, \qquad z = (\tau + \rho\eta)x + \rho cu + abv$$

for some $u, v \in \mathbb{Z}$, so

$$\begin{pmatrix} 1 \\ \eta \\ \tau + \rho\eta \end{pmatrix}, \qquad \begin{pmatrix} 0 \\ c \\ \rho c \end{pmatrix}, \qquad \begin{pmatrix} 0 \\ 0 \\ ab \end{pmatrix}$$

form a basis for the lattice Λ of determinant abc. The compact, symmetric, convex body

$$[-\sqrt{bc}, \sqrt{bc}] \times [-\sqrt{ac}, \sqrt{ac}] \times [-\sqrt{ab}, \sqrt{ab}]$$

has volume

$$8abc = 2^3 \det(\Lambda)$$

so, by strong Minkowski, it contains a non-zero element $(x, y, z) \in \Lambda$.

Now

$$x^2 \leqslant bc, \qquad y^2 \leqslant ac, \qquad z^2 \leqslant ab.$$

If $x^2 = bc$ then, since b, c are coprime and squarefree, we must have $b = c = 1$, and our equation has the solution $(0, 1, 1)$. We may therefore assume instead that $x^2 < bc$.

Next, suppose $z^2 = ab$. Then $a = b = 1$. In this case -1 is a quadratic residue modulo c, so c can't have any prime factors that are 3 mod 4, so c is a sum of two squares. Thus, we may also assume that $z^2 < ab$.

Now $ax^2+by^2-cz^2$ is a multiple of abc and lies in the interval $(-abc, 2abc)$, so it's either 0 or abc. If it's zero, then (x, y, z) solves the equation, and if

$$ax^2 + by^2 - cz^2 = abc$$

then

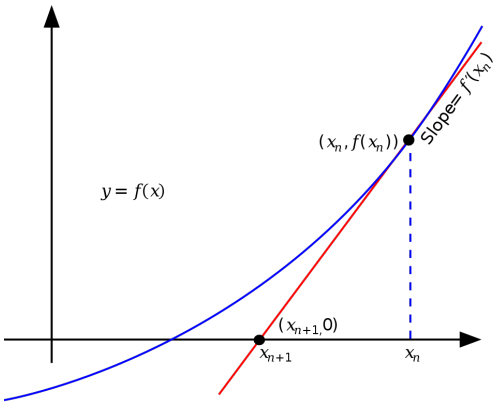
$$a(xz + by)^2 + b(yz - ax)^2 - c(z^2 + ab)^2 = 0.$$

□

2.6 Hensel's lemma

If a diophantine equation has an integer solution, then it's also soluble modulo any positive integer. By the Chinese remainder theorem, the latter is equivalent to solubility modulo any prime power. However, a root modulo a prime p can often be upgraded to a root modulo any given power of p.

Let's start with a close analogy. Let f be a real function on an interval, with continuous second derivative. Given a good initial estimate for a root of f, the Newton–Raphson method constructs a sequence of points whose distance to the root decreases rapidly to zero.



Newton–Raphson method:

1. Choose x_1 very close to a root of f.
2. For $n \in \mathbb{N}$, let $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$.

Let p be prime. Recall that the *p-adic order* of $n \in \mathbb{Z}$ is

$$\nu_p(n) = \sup\{k : p^k \mid n\}.$$

The *p-adic absolute value* of n is

$$|n|_p = p^{-\nu_p(n)}.$$

Thus, being small means being divisible by a higher power of p, and being close means being congruent modulo a high power of p. Finding smaller and smaller values of a polynomial means solving it modulo higher and higher powers of p.

Lemma 2.6.1 (Hensel's lemma)**.** *Let $f(x) \in \mathbb{Z}[x]$. Suppose $k, n, x \in \mathbb{Z}$ satisfy*

$$f(x) \equiv 0 \bmod p^n, \qquad p^k \| f'(x), \qquad n \geqslant 2k+1.$$

Then there exists $y \equiv x \bmod p^{n-k}$ such that

$$f(y) \equiv 0 \bmod p^{n+1}, \qquad p^k \| f'(y).$$

Remark 2.6.2. (a) We can iterate to find a root modulo any power of p.

(b) It's most common to apply this with $k = 0$. We find that if $f(x) \equiv 0 \bmod p^n$ and $p \nmid f'(x)$ then there exists $y \in \mathbb{Z}$ such that $f(y) \equiv 0 \bmod p^{n+1}$ and $p \nmid f'(y)$.

(c) Applying the lemma with $k = 1$, we find that if an odd number is a quadratic residue modulo 8 then it's a quadratic residue modulo any power of 2.

Example 2.6.3. As $\left(\frac{2}{7}\right) = 1$, we can apply Hensel's lemma to $x^2 - 2$, and find that 2 is a quadratic residue modulo any power of 7. Can you see explicitly how it's a quadratic residue modulo 49?

Proof. Write

$$y = x + zp^{n-k},$$

where z is an integer to be determined. It follows from Taylor's theorem that

$$f(y) \equiv f(x) + f'(x)zp^{n-k} \mod p^{2n-2k}.$$

As $2n - 2k \geqslant n + 1$, we thus have

$$f(y) \equiv f(x) + f'(x)zp^{n-k} \mod p^{n+1}.$$

Next, let $a, b \in \mathbb{Z}$ with

$$f'(x) = ap^k, \qquad f(x) = bp^n.$$

Then $p \nmid a$ and

$$f(y) \equiv (az + b)p^n \mod p^{n+1}.$$

We choose $z \equiv -a^{-1}b \mod p$ to ensure that $f(y) \equiv 0 \mod p^{n+1}$.

As $y \equiv x \mod p^{n-k}$, we have $f'(y) \equiv f'(x) \mod p^{n-k}$. Hence $f'(y) \equiv f'(x) \mod p^{k+1}$, so as $p^k \| f'(x)$ we must also have $p^k \| f'(y)$. □

To complete the analogy, these roots need to converge to a limit.

Example 2.6.4. Completing the rationals with respect to $|\cdot|$ forms the reals, where every Cauchy sequence has a limit.

This requires us to complete the integers with respect to the the p-adic absolute value, forming the p-adic integers. In the same way, completing the rationals with respect to $|\cdot|_p$ gives rise to the p-adic numbers.

2.7 Waring's problem

For $k \in \mathbb{N}$, denote by $g(k)$ the least $s \in \mathbb{N}$ such that if $n \in \mathbb{N}$ then there exist $x_1, \ldots, x_s \in \mathbb{Z}_{\geqslant 0}$ such that

$$x_1^k + \cdots + x_s^k = n.$$

By Lagrange's four-square theorem and Legendre's three-square theorem, we have $g(2) = 4$. Waring (1770) conjectured that $g(k) < \infty$ for all k. This was finally proved by Hilbert in 1909, using polynomial identities, but with poor bounds on $g(k)$.

Theorem 2.7.1 (Refinement of Liouville, 1859)**.** *We have* $g(4) \leqslant 50$.

Proof. Using your favourite computer algebra software, you can check that

$$6\left(\sum_{i=1}^{4} a_i^2\right)^2 = \sum_{1\leqslant i<j\leqslant 4} \left((a_i+a_j)^4 + (a_i-a_j)^4\right).$$

By Lagrange's four-square theorem, this enables us to write any number of the form $6A^2$ as a sum of twelve biquadrates. By Lagrange's four-square theorem, we can write any $N \in \mathbb{Z}_{\geqslant 0}$ as $A_1^2 + \cdots + A_4^2$, so any number of the form $6N$ is now a sum of 48 biquadrates. For $n \geqslant 81$, one can write $n = 6N + r$ with $r = 0, 1, 2, 81, 16, 17$, where r is the sum of two biquadrates. One can check the cases $n \leqslant 80$ separately. □

Example 2.7.2. How many k^{th} powers are needed to represent

$$n_0 = 2^k\lfloor (3/2)^k \rfloor - 1 \qquad ?$$

As $n_0 < 3^k$, we can only use 2^k and 1^k, and the most efficient way is to use $\lfloor (3/2)^k \rfloor - 1$ copies of 2^k together with $2^k - 1$ copies of 1^k. Thus

$$g(k) \geqslant 2^k + \lfloor (3/2)^k \rfloor - 2.$$

In fact, with $\{y\} = y - \lfloor y \rfloor$ being the fractional part function, we know that

$$g(k) = 2^k + \lfloor (3/2)^k \rfloor - 2$$

as long as

$$2^k\{(3/2)^k\} + \lfloor (3/2)^k \rfloor \leqslant 2^k,$$

and that the latter inequality has at most finitely many exceptions (Mahler, 1957). The inequality has been confirmed for $k \leqslant 4.7 \times 10^8$ (Kubina and Wunderlich, 1990).

What if we were to exclude small values of n? This brings us to the modern formulation of Waring's problem. For $k \in \mathbb{N}$, denote by $G(k)$ the least $s \in \mathbb{N}$ such that if $n \in \mathbb{N}$ is sufficiently large then there exist non-negative integers $x_1, \ldots, x_s$ such that

$$x_1^k + \cdots + x_s^k = n.$$

Note from the definitions that

$$G(k) \leqslant g(k) \qquad (k \in \mathbb{N}).$$

By Lagrange's four-square theorem and Legendre's three-square theorem, we have

$$G(2) = 4 = g(2).$$

In general $G(k)$ is much smaller than $g(k)$.

Linnik (1941) showed that $G(3) \leqslant 7$. Your second favourite lecturer, with computer assistance, was able to determine precisely which integers are a sum of at most seven positive cubes.

Theorem 2.7.3 (Siksek, 2016)**.** *Every integer greater than 454 is a sum of seven non-negative cubes.*

Theorem 2.7.4. *For $k \geqslant 2$ we have $G(k) \geqslant k + 1$.*

Proof. Let $A(N)$ be the number of natural numbers $n \leqslant N$ that are of the form

$$n = x_1^k + \cdots + x_k^k \qquad (x_i \in \mathbb{Z}_{\geqslant 0}). \tag{2.1}$$

Then $A(N) \leqslant B(N)$, where $B(N)$ counts $(x_1, \ldots, x_k) \in \mathbb{Z}^k$ such that

$$0 \leqslant x_1 \leqslant x_2 \leqslant \ldots \leqslant x_k \leqslant N^{1/k}.$$

We compute that

$$\begin{aligned} B(N) &= \sum_{x_k=0}^{\lfloor N^{1/k} \rfloor} \cdots \sum_{x_2=0}^{\lfloor N^{1/k} \rfloor} \sum_{x_1=0}^{x_2} 1 \\ &= (\lfloor N^{1/k} \rfloor + 1)^{k-2} \sum_{x_2=0}^{\lfloor N^{1/k} \rfloor} (x_2 + 1) \\ &= (\lfloor N^{1/k} \rfloor + 1)^{k-2} \frac{(\lfloor N^{1/k} \rfloor + 1)(\lfloor N^{1/k} \rfloor + 2)}{2} \sim \frac{N}{2} \qquad (N \to \infty). \end{aligned}$$

Thus, if N is sufficiently large, then

$$B(N) \leqslant \frac{2}{3} N.$$

Assume for a contradiction that $G(k) \leqslant k$. Then all but a finite number of $n \in N$ are representable as a sum of k non-negative k^{th} powers. Let E be the number of these exceptions. Then for all sufficiently large N we have

$$N - E = A(N) \leqslant B(N) \leqslant \frac{2}{3} N.$$

Now $N/3 \leqslant E$ for all sufficiently large N, contradiction. Therefore we must instead have

$$G(k) \geqslant k+1.$$

□

Stronger lower bounds are known for some specific values of k. For example, if $k = 2^m \geqslant 4$ then

$$G(k) \geqslant 4k.$$

There are numerous upper bounds that are much more involved. The record is held by Brüdern and Wooley (2022), who showed that

$$G(k) \leqslant \lceil k(\log k + 4.20032) \rceil \qquad (k \in \mathbb{N}).$$

2.8 Diophantine approximation

Diophantine approximation quantifies the fact that $\mathbb{Q}$ is dense in $\mathbb{R}$. Close rational approximations to a real number can be found, for example, by truncating its decimal expansion. More generally, to approximate $\alpha \in \mathbb{R}$, one can choose the denominator q arbitrarily, and take the closest numerator to $q\alpha$.

Lemma 2.8.1. *Let $\alpha \in \mathbb{R}$. Then there exists $q \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that*

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{2q}.$$

One can do better, in the sense that a closer approximation can be found, considered in terms of the size of the denominator.

Theorem 2.8.2 (Dirichlet's approximation theorem)**.** *Let $\alpha \in \mathbb{R}$ and $Q \in \mathbb{N}$. Then there exist $a, q \in \mathbb{Z}$ such that*

$$1 \leqslant q \leqslant Q, \qquad \left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}.$$

Proof. We wish to find a positive integer $q \leqslant Q$ such that

$$\|q\alpha\| < Q^{-1},$$

where $\|\theta\| = \min_{a\in\mathbb{Z}} |\theta - a|$. For $u = 0, 1, \ldots, Q-1$, define $I_u = \left[\frac{u}{Q}, \frac{u+1}{Q}\right)$. By the pigeonhole principle, some I_u must contain $\{i\alpha\}, \{j\alpha\}$, for some $0 \leqslant i < j \leqslant Q$. For $q = j - i$, we have

$$q\alpha - (\{j\alpha\} - \{i\alpha\}) = \lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor \in \mathbb{Z},$$

so

$$\|q\alpha\| \leqslant |\{j\alpha\} - \{i\alpha\}| < Q^{-1}.$$

□

Corollary 2.8.3. *If $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ then there are infinitely many reduced fractions a/q such that*

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}.$$

Proof. Given $Q \in \mathbb{N}$, Dirichlet's approximation theorem gives $a, q \in \mathbb{Z}$ such that $1 \leqslant q \leqslant Q$ and $|\alpha - a/q| < 1/(qQ)$. By putting a/q in lowest terms, we may assume that $(a, q) = 1$.

Assume for a contradiction that there are only finitely many such reduced fractions, namely

$$\frac{a_1}{q_1}, \ldots, \frac{a_n}{q_n}.$$

As $\alpha \notin \mathbb{Q}$, we have

$$\alpha - \frac{a_i}{q_i} \neq 0 \qquad (1 \leqslant i \leqslant n).$$

Thus, there exists $Q \in \mathbb{N}$ such that

$$\left|\alpha - \frac{a_i}{q_i}\right| > \frac{1}{Q} \qquad (1 \leqslant i \leqslant n).$$

By Dirichlet's approximation theorem, there exist coprime $a, q \in \mathbb{Z}$ such that

$$1 \leqslant q \leqslant Q, \qquad \left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ} \leqslant \frac{1}{Q} \qquad (1 \leqslant q \leqslant Q).$$

Now a/q is a reduced fraction with $|\alpha - a/q| < q^{-2}$, and $a/q \neq a_i/q_i$ for $i = 1, 2, \ldots, n$, contradiction. □

The 'best approximations' to a real numbers can be computed using continued fractions. They can be used to slightly refine the estimate above.

Theorem 2.8.4 (Hurwitz, 1891)**.** *If $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ then there are infinitely many reduced fractions a/q such that*

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

In the case $\alpha = \frac{1+\sqrt{5}}{2}$, the constant $\sqrt{5}$ can't be replaced by a larger one.

An *algebraic number* is the root of a non-zero polynomial with rational coefficients. Its *degree* is the least degree of such a polynomial. Algebraic numbers are complex in general, but we'll consider real algebraic numbers.

Theorem 2.8.5 (Liouville, 1844)**.** *Let $\alpha \in \mathbb{R}$ be algebraic of degree $n \geqslant 2$. Then there exists $c = c(\alpha) > 0$ such that if $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ then*

$$\left|\alpha - \frac{a}{q}\right| > \frac{c}{q^n}.$$

Proof. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n such that $f(\alpha) = 0$. We may assume that $|\alpha - a/q| \leqslant 1$. By the mean value theorem, we have

$$|f(a/q)| = |f(\alpha) - f(a/q)| \leqslant A|\alpha - a/q|,$$

where

$$A = \max\{|f'(x)| : |x - \alpha| \leqslant 1\}.$$

As $\alpha \notin \mathbb{Q}$, we have $f(a/q) \neq 0$, for otherwise

$$\frac{f(x)}{x - a/q} \in \mathbb{Q}[x] \setminus \{0\}$$

would be a lower-degree polynomial vanishing at α. As $q^n f(a/q) \in \mathbb{Z}$, we thus have

$$1 \leqslant q^n|f(a/q)| \leqslant Aq^n|\alpha - a/q|.$$

□

Liouville's theorem was refined by Thue (1909) and Siegel (1921), before Roth finally attained the optimal exponent.

Theorem 2.8.6 (Roth, 1955)**.** *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be algebraic, and let $\varepsilon > 0$. Then there exists $c = c(\alpha, \varepsilon) > 0$ such that if $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ then*

$$\left|\alpha - \frac{a}{q}\right| > \frac{c}{q^{2+\varepsilon}}.$$