Introduction to Number Theory

Payman Eskandari

Winter 2025-2026

These notes do not substitute for lectures. Not everything we say in class will be included here (e.g., some details may be missing).

There will almost surely be some typos. If you catch typos, please send them to me.

Contents

0 Introduction: What is number theory? 3
- 0.1 Problems related to the distribution of prime numbers . . . 3
  - 0.1.1 The prime number theorem . . . 3
  - 0.1.2 Twin primes . . . 3
  - 0.1.3 The Goldbach problem . . . 4
- 0.2 Diophantine equations . . . 4
- 0.3 Questions related to rationality/irrationality . . . 4

1 Week 1: Divisibility and prime numbers 5
- 1.1 Definitions and the statement of the fundamental theorem . . . 5
- 1.2 Division algorithm and the greatest common divisor . . . 7
- 1.3 Euclidean algorithm . . . 8
- 1.4 Euclid's first theorem and the uniqueness part of the FTA . . . 9

2 Week 2: Some applications of the FTA and on the infinitude of primes 10
- 2.1 First application: GCD and LCM in terms of prime factorizations . . . 10
- 2.2 Second application: Some irrationality proofs . . . 11
- 2.3 Euclid's proof of infinitude of primes . . . 12
- 2.4 Euclid's proof of infinitude of primes revisited . . . 12
- 2.5 Second proof of infinitude of primes and a better lower bound for $\pi(x)$ . . . 13
- 2.6 Euler's proof of infinitude of primes . . . 14
- 2.7 Primes in arithmetic progressions . . . 14

3 Week 3: Linear Diophantine equations, basics of congruence, and divisibility rules 16
- 3.1 Linear Diophantine equations . . . 16
- 3.2 Congruence: Definition and basic properties . . . 18
- 3.3 Application: Divisibility rules . . . 21

4 Week 4: Congruence equations, units, and the Chinese remainder theorem 23
4.1 Cancellation property for congruences . . . 23
4.2 What is a congruence equation? . . . 24
4.3 Linear congruences . . . 24
4.4 Multiplicative inverses and units mod m . . . 25
4.5 Finding multiplicative inverses . . . 26
4.6 Systems of linear congruences and the Chinese remainder theorem . . . 27

5 Week 5: Chinese remainder theorem continued and residue classes 28
5.1 The Chinese remainder theorem continued . . . 28
5.2 Residue classes . . . 30

6 Week 6: Complete sets of residues mod m, Euler's φ function, Fermat's and Euler's theorems 31
6.1 Complete sets of residues mod m, coprime to m, and Euler's function . . . 31
6.2 How to compute $\varphi(m)$ . . . 33
6.3 Proof of multiplicativity of φ . . . 34
6.4 Euler's and Fermat's theorems . . . 36

7 Week 7: Order mod m, Wilson's theorem, quadratic residues 39
7.1 Order mod m . . . 39
7.2 Wilson's theorem . . . 40
7.3 Quadratic residues: The statement of the problem and the definitions . . . 41
7.4 Quadratic residues: The statements of the main results . . . 43
7.5 Quadratic residues: Examples . . . 44

8 Week 8: Quadratic residues: Proofs of the main results I 46
8.1 Multiplicativity of the Legendre symbol . . . 47
8.2 Euler's criterion and the determination of $\left(\frac{-1}{p}\right)$ . . . 48

9 Week 9: Quadratic residues: Proofs of the main results II 50
9.1 Gauss' lemma . . . 50
9.2 The proof of the characterization of $\left(\frac{2}{p}\right)$ . . . 52

10 Week 10: Proof of quadratic reciprocity, some applications, sums of squares 52
10.1 The proof of the quadratic reciprocity . . . 52
10.2 Application: Infinitude of primes of the form $4k+1$ . . . 55
10.3 Application to Diophantine equations . . . 56
10.4 Sums of squares . . . 57

11 Week 11: Sums of squares (continued), Pythagorean triples 58
11.1 Sums of squares (continued) . . . 58
11.2 Sums of squares (continued): Proof of Fermat's theorem . . . 60
11.2.1 Step 1 . . . 60
11.2.2 Step 2: The descent procedure . . . 61
11.3 Pythagorean triples I: The elementary approach . . . 63

11.4 Pythagorean triples II: The connection to rational points on the unit circle . . 65

12 Week 12: Rational points on conics **66**
12.1 Rational points on the unit circle 66
12.2 Rational points on conics 69

0 Introduction: What is number theory?

Number theory is the branch of mathematics whose goal is to study the natural numbers. It is essentially as old as mathematics itself.

Gauss famously said: "Mathematics is the queen of the sciences, and number theory is the queen of mathematics."

Below we discuss some examples of the kind of problems number theory is concerned with.

0.1 Problems related to the distribution of prime numbers

Euclid (around 300 BC) proved that there are infinitely prime numbers. This leads one to ask questions about the distributions of primes. For example, how often do primes occur? Is there a pattern in the way they occur? We will mention three famous problems in this direction.

0.1.1 The prime number theorem

Given any $x \geq 0$, let $\pi(x)$ be the number of prime numbers $\leq x$. By Euclid, $\pi(x) \to \infty$ as $x \to \infty$. The natural question is:

Problem 1. Estimate $\pi(x)$.

An answer to this is given by

Theorem 2 (Prime number theorem, Haramard and de la Vallée Poussin, 1896)**.** *We have*

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

Note that here and elsewhere, log means the natural logarithm (i.e., what you write as ln in calculus).

0.1.2 Twin primes

It is easy to see that the only two primes of the form $n, n+1$ (i.e., whose difference is 1) are 2 and 3. Next, we may ask about primes of the form $n, n+2$. These are called *twin primes*. Examples of twin primes are $\{3,5\}$, $\{5,7\}$, $\{11,13\}$ and $\{17,19\}$.

Problem 3. Are there infinitely many twin primes?

To date, this is an open problem! The answer is predicted by the following conjecture, which was formulated around 1850 (if not before then) and remains open to date.

Conjecture 4 (Twin primes conjecture)**.** There exist infinitely many twin primes.

0.1.3 The Goldbach problem

Experiments suggest that every even integer greater than 2 could be a sum of two primes: 4=2+2, 6=3+3, 8=3+5, 10=5+5, 12=5+7, 14=7+7, etc. This lead to the famous

Conjecture 5 (Goldbach conjecture, 1742)**.** Every even integer greater than 2 is a sum of two prime numbers.

The conjecture remains open to date. It has been numerically checked for even integers up to 4×10^{18}.

These problems are only the tip of the iceberg. Even with answers to these, many many questions would remain.

0.2 Diophantine equations

Diophantine equations are polynomial equations with integral (i.e., integer) coefficients, where one is interested in solutions in the integers or rational numbers. They date back to ancient Greece, at least.

For example, consider the equation

$$x^2 + y^2 = z^2.$$

How many solutions are there in $\mathbb{Z}$? In other words, how many right triangles are there with integer side lengths? Solutions to this equation are called *Pythagorean triples*. Some examples are $(x, y, z) = (3, 4, 5)$ and $(x, y, z) = (5, 12, 13)$. It has been known since the ancient times that there are infinitely many Pythagorean triples (this will be one of our topics in the course!).

Let's "slightly" tweak the equation. Consider

$$x^3 + y^3 = z^3.$$

How many solutions in $\mathbb{Z}$ does this equation have? It turns out that this is now a completely different question to the Pythagorean question. Fermat conjectured around 1637 the following statement, which is famously known as *Fermat's last theorem*, although Fermat never provided a proof for it and so it was really a conjecture.

Conjecture 6. (Fermat's last "theorem") Let n be an integer ≥ 3. There are no positive integers x, y, z such that

$$x^n + y^n = z^n.$$

This was finally proved by Andrew Wiles in 1994. It was the culmination of complex mathematical theories developed over a number of centuries.

Diophantine equations continue to remain a very active area of mathematics.

0.3 Questions related to rationality/irrationality

Recall that a real number is called rational if it can be expressed as a fraction a/b for some integers a, b. Real numbers that are not rational are called irrational. Questions about rationality of specific numbers are part of number theory.

The ancient Greek know since shortly after Pythagoras (around 500 BC) that $\sqrt{2}$ is irrational. Irrationality of numbers of the form $\sqrt{N}$ for non-square N *could* have already

been known by Euclid, in that it doesn't require more sophisticated techniques than what Euclid knew already. However, irrationality of numbers such as π, e were not known until the 18th century:

- 1737: Euler was the first to prove irrationality of e.
- 1761: Lambert proved irrationality of π.
- 1882: Lindemann proved that π is *transcendental*. In particular, all powers of π are irrational.

There are many fascinating open problems in this direction. We will give one story leading to many such problems.

For $s > 1$, let

$$\zeta(s) \;=\; \sum_{n=1}^{\infty} \frac{1}{n^s} \;=\; 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{3^s} + \cdots .$$

You may remember from calculus that the sum converges for $s > 1$. At $s = 1$, this is called the harmonic series and it diverges. But for any $s > 1$, $\zeta(s)$ is a real number > 1. These were established by Pietro Mengoli in 1600's. Mengoli posed the so-called *Basel problem* in 1650: Find the exact sum

$$\zeta(2) = 1 + 1/4 + 1/9 + 1/25 + \cdots .$$

The problem was finally answered by a young Euler in the way of the following remarkable formula:

Theorem 7 (Euler, 1735)**.**

$$\zeta(2) = \pi^2/6$$

Euler also evaluated $\zeta(4), \zeta(6)$, etc. He showed that

$$\zeta(2k) = \pi^{2k} \cdot \text{a rational number.}$$

Combining with Lindemann's theorem, all of numbers $\zeta(2), \zeta(4), \zeta(6)$, etc. are irrational.

The story of the *odd zeta values* $\zeta(3), \zeta(5), \zeta(7)$, etc. is completely different. In particular, we don't expect there to be a similar relation between odd zeta values and powers of π (as there is for even zeta values). There are no closed form values known, and to date, very very little is known about their irrationality. It took until 1979 that finally it was proved that:

Theorem 8 (Ápery 1979)**.** $\zeta(3)$ *is irrational.*

$\zeta(3)$ is the only odd zeta value whose irrationality has been proved. It is conjectured that all the odd zeta values are irrational (and in fact, a much stronger statement is expected). But this seems to be outside the reach of current mathematics.

1 Week 1: Divisibility and prime numbers

1.1 Definitions and the statement of the fundamental theorem

We denote the set of all integers by $\mathbb{Z}$. The set of all positive (resp. nonnegative) integers is denoted by $\mathbb{Z}_{>0}$ (resp. $\mathbb{Z}_{\geq 0}$).

Definition 1.1 (Divisibility)**.** Let $a, b \in \mathbb{Z}$. We say b divides a (or a is divisible by b, or b is a divisor of a) and write $b \mid a$ if there exists an integer k such that $a = bk$.

For example, 2 divides 6.

Exercise 1.1. List all positive divisors of 12.

Exercise 1.2. Let $a \in \mathbb{Z}$.

(a) Show that $a \mid a$.

(b) Show that $a \mid 0$.

(c) Show that $1 \mid a$.

(d) Show that if $a \mid 1$, then $a = \pm 1$.

Proposition 1.2. *Let $a, b, c \in \mathbb{Z}$. Then:*

(a) *If $c \mid b$ and $b \mid a$, then $c \mid a$.*

(b) *If $c \mid b$ and $c \mid a$, then $c \mid a + b$.*

(c) *If $b \mid a$, then $b \mid an$ for every $n \in \mathbb{Z}$.*

(d) *If $c \mid a$ and $c \mid b$, then $c \mid am + bn$ for every $m, n \in \mathbb{Z}$.*

Proof. See your class notes. You probably also saw these in your Discrete Math course. □

Definition 1.3 (Prime numbers)**.** An integer p is called a prime number if it satisfies the following two conditions:

(i) $p > 1$

(ii) If $p = ab$ for some $a, b \in \mathbb{Z}_{>0}$, then either $a = 1$ or $b = 1$. (Equivalently, the only positive divisors of p are 1 and p.)

The first five prime numbers are 2,3,5,7,11. An integer > 1 that is not prime is called *composite*.

Proposition 1.4. *Every integer ≥ 2 can be expressed as a product of prime numbers.*

Proof. The proof is by strong induction. The number 2 is prime itself (and hence a product of primes with one factor). Suppose $n \geq 2$ and that all the integers $2, \ldots, n$ are products of primes. We show that $n + 1$ is also a product of primes.

If $n+1$ is prime, we are done. Suppose $n+1$ is not prime. Then by definition, there exist integers a, b with $1 < a, b < n + 1$ such that $n + 1 = ab$. By the induction hypothesis, both a and b are products of primes. Combining the two factorizations, $n + 1$ is also a product of primes. □

For example,

$$24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3$$

and we have managed to write 24 as a product of primes.

For convenience, we define the empty product to be 1. Then the number 1 is also a product of primes (well, an empty collection of them!), and the last proposition says every positive integer is a product of primes. Note that this proposition only asserts existence of a prime factorization. One of Euclid's impressive contributions was to prove that this factorization is unique:

Theorem 1.5 (Euclid)**.** (The Fundamental Theorem of Arithmetic (FTA)) *Every positive integer is a product of primes. Moreover, the prime factorization of any positive integer is unique up to rearranging the prime factors.*

The uniqueness assertion is quite deeper than the existence assertion. We need to develop some tools first.

Exercise 1.3. Let p and q be prime numbers. Show that if $p \mid q$, then $p = q$.

1.2 Division algorithm and the greatest common divisor

Proposition 1.6 (Division algorithm)**.** *Let $a, b \in \mathbb{Z}$ and $b > 0$. Then there exist unique integers q, r such that*

$$a = qb + r$$

and

$$0 \leq r < b.$$

(The number r is called the remainder of a in division by b.)

Proof. For existence, let q be such that

$$qb \leq a < (q+1)b.$$

Set $r = a - qb$. Both conditions are met.

For uniqueness, suppose q, r as well as q', r' satisfies the two conditions. Then

$$qb + r = a = q'b + r',$$

so that

$$(q - q')b = r' - r.$$

Since $0 \leq r, r' < b$, we have $-b < r - r' < b$. It follows from the above equation that $q - q' = 0$ and $r' - r = 0$. □

Let a, b be integers with a or b nonzero. The greatest common divisor of a, b (denoted by $\gcd(a, b)$) is what the term suggests. It is characterized by two properties: (i) $\gcd(a, b)$ is a common divisor of (i.e., divides both) a and b, and (ii) for every common divisor c of a and b, we have $c \leq \gcd(a, b)$.

Lemma 1.7. *Show that*

$$\gcd(a, b) = \gcd(b, a + bm)$$

for every integer m.

Proof. We did this in class. See your notes. □

Exercise 1.4. Let a, b be integers, not both zero. Let $d = \gcd(a, b)$. Show that $\gcd(a/d,\ b/d) = 1$.

Recall that two integers a, b are called relatively prime (or coprime) if $\gcd(a, b) = 1$.

1.3 Euclidean algorithm

Given a and b, their greatest common divisor can be calculated efficiently using iterations of the division algorithm. This process is called the Euclidean (or Euclid's) algorithm. We may assume that $a \geq b > 0$ (other cases are either trivial or can be reduced to this). Then by the division algorithm, there are integers r_1, q_1 such that

$$a = bq_1 + r_1 \qquad (0 \leq r_1 < b).$$

If $r_1 \neq 0$, again by the division algorithm (this time dividing b by r_1) we know there are integers r_2, q_2 such that

$$b = r_1 q_2 + r_2 \qquad (0 \leq r_2 < r_1).$$

Continuing in the same fashion, in the i^{th} step, having already found $r_1, q_1, \ldots, r_{i-1}, q_{i-1}$, if $r_{i-1} \neq 0$, dividing r_{i-2} by r_{i-1} we find r_i, q_i such that

$$r_{i-2} = r_{i-1} q_i + r_i \qquad (0 \leq r_i < r_{i-1}).$$

We stop when we get a zero remainder. The non-negative integers $b, r_1, r_2, \ldots$ are strictly decreasing, so the procedure must stop at some point, i.e., eventually there will be k such that $r_k = 0$. Thus

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1} \\ r_{k-2} &= r_{k-1} q_k. \end{aligned} \tag{1.1}$$

We claim that $r_{k-1} = \gcd(a, b)$. Indeed, by iterations of Lemma 1.7 we have

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-1}, r_k) = r_{k-1}$$

because $r_k = 0$.

Example 1.8. Let us find $\gcd(12345, 1745)$:

$$12345 = 1745 \cdot 7 + 130, \quad 1745 = 130 \cdot 13 + 55, \quad 130 = 55 \cdot 2 + 20, \quad 55 = 20 \cdot 2 + 15$$

$$20 = 15 \cdot 1 + 5, \quad 15 = 5 \cdot 3,$$

and hence $\gcd(12345, 1745) = 5$.

Working through the equations of (1.1) backwards, we obtain the following fundamental result:

Proposition 1.9. *Let a, b be integers not both of which are zero. Then there exist integers x, y such that*

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

Example 1.10. In Example 1.8 we computed that $\gcd(12345, 1745) = 5$. Working through the computations of the example backwards, we have

$$\begin{aligned} 5 = 20 - 15 \cdot 1 &= 20 - (55 - 20 \cdot 2) \cdot 1 = -55 \cdot 1 + 20 \cdot 3 \\ &= -55 \cdot 1 + (130 - 55 \cdot 2) \cdot 3 = 130 \cdot 3 - 55 \cdot 7 \\ &= 130 \cdot 3 - (1745 - 130 \cdot 13) \cdot 7 = -1745 \cdot 7 + 130 \cdot 94 \\ &= -1745 \cdot 7 + (12345 - 1745 \cdot 7) \cdot 94 = 12345 \cdot 94 - 1745 \cdot 665. \end{aligned}$$

Thus $x = 94$ and $y = -665$ is a solution to $12345x + 1745y = 5$.

The process of working through the computations of the Euclidean algorithm backwards to write $\gcd(a, b)$ as a linear combination of a and b is sometimes called the *extended* Euclidean algorithm.

1.4 Euclid's first theorem and the uniqueness part of the FTA

The heart of the uniqueness part of the fundamental theorem of arithmetic (Theorem 1.5) is the following:

Theorem 1.11 (Euclid, around 300BC)**.** *Let p be a prime number and $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. Suppose $p \nmid a$. We will show that $p \mid b$. Since $p \nmid a$, we have $\gcd(a, p) = 1$. Thus by Proposition 1.9 there exist integers x, y such that $ax + py = 1$. Multiplying by b, we get

$$abx + pby = b.$$

On recalling $p \mid ab$ we see that the left hand side is a multiple of p. Thus $p \mid b$. □

By induction on the number of factors we obtain the following more general statement:

Corollary 1.12. *If p is a prime number, $a_1, \ldots, a_k$ are integers and p divides the product $a_1 \cdots a_k$, then p divides a_i for some $1 \leq i \leq k$.*

From this it is easy to deduce the uniqueness part of the fundamental theorem, as we do now.

Completion of the proof of the fundamental theorem of arithmetic (Theorem 1.5). Existence of prime factorizations was already proved in Proposition 1.4. It remains to prove the uniqueness.

Suppose an integer n has two prime factorizations

$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}, \tag{1.2}$$

where $p_1 < p_2 < \cdots < p_k$ and $q_1 < q_2 < \cdots < q_l$ are primes and the a_i and the b_i are positive integers. We need to show that $k = l$, $p_i = q_i$ and $a_i = b_i$ for all i.

Take p be one of the p_i. Then p divides the left hand and hence the right hand side of (1.2). By Theorem 1.11 (or rather, its more general form recorded as Corollary 1.12) it follows that p divides q_i for some $1 \leq i \leq l$. Since p and q_i are prime, we get $p = q_i$. That is, every prime in the left hand side of (1.2) appears also in the right hand side. By a similar argument, every prime on the right hand side of the equation also appears on the left side. That is, the set of primes $\{p_1, \ldots, p_k\}$ and $\{q_1, \ldots, q_l\}$ are equal. It follows that $k = l$ and $p_i = q_i$ for all i (since we indexed our primes in an increasing order). So (1.2) now reads

$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

It remains to show that the exponents match. Fix i and suppose $a_i < b_i$. Divide both sides of the last equation by $p_i^{a_i}$. Then the right hand side is still a multiple of p_i, so that the left hand side (where no longer the factor $p_i^{a_i}$ appears) is a multiple of p_i. By Corollary 1.12, p_i must divide one of $p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_k$, which is a contradiction. □

Exercise 1.5. Let m, a and b be integers. Show that if $m \mid ab$ and $\gcd(m, a) = 1$, then $m \mid b$. (Hint: Imitate the proof of Theorem 1.11.)

Exercise 1.6. Let m, m', a be integers. Suppose m and m' both divide a and $\gcd(m, m') = 1$. Show that mm' divides a. (Hint: Write $a = mk$. We know m' divides a and $\gcd(m', m) = 1$. Use the last exercise.)

Exercise 1.7. Let a, b be nonzero integers. Show that $\operatorname{lcm}(a, b) \mid ab$.

Exercise 1.8. Let a, b be positive integers. Show that $\gcd(a, b) = 1$ if and only if a and b do not have any common prime divisors.

Exercise 1.9. Let m, n, a be positive integers. Show that

$$\gcd(a, mn) = 1 \quad \Longleftrightarrow \quad \gcd(a, m) = \gcd(a, n) = 1.$$

2 Week 2: Some applications of the FTA and on the infinitude of primes

2.1 First application: GCD and LCM in terms of prime factorizations

Recall that the least common multiple of two integers a, b, denoted by $\operatorname{lcm}(a, b)$ is characterized by the following properties: (i) $\operatorname{lcm}(a, b)$ is an integer ≥ 0 which a common multiple of (i.e., it is divisible by both) a and b, and (ii), for every common multiple l of a and b, we have $\operatorname{lcm}(a, b) \leq l$.

All assertions of the next proposition are immediate consequences of the fundamental theorem of arithmetic.

Proposition 2.1. *Let $p_1, \ldots, p_k$ be distinct prime numbers. Let $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$, where the α_i and β_i are non-negative integers.*

(a) *An integer d is a positive divisor of a if and only if $d = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ for some integers $\gamma_1, \ldots, \gamma_k$ with $0 \le \gamma_i \le \alpha_i$ for $1 \le i \le k$. In particular, the number of positive divisors of a is*

$$\prod_{i=1}^{k} (\alpha_i + 1) \;=\; (\alpha_1 + 1) \cdots (\alpha_k + 1).$$

(b) *We have*

$$\gcd(a,b) = \prod_{i=1}^{k} p_i^{\min(\alpha_i\,,\,\beta_i)}, \qquad \operatorname{lcm}(a,b) = \prod_{i=1}^{k} p_i^{\max(\alpha_i\,,\,\beta_i)}.$$

The formulas in part (b) have the following consequence:

Corollary 2.2. *For every positive integers a, b,*

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab.$$

2.2 Second application: Some irrationality proofs

Recall that a real number α is rational if there exist integers a, b with $b \neq 0$ such that $\alpha = a/b$. A real number that is not rational is called irrational. The set of all rational numbers is denoted by $\mathbb{Q}$.

Proposition 2.3. *Let $m \ge 2$ be an integer. Let N be a positive integer that is not an m-th power of any integer, i.e., $N \neq N_1^m$ for any $N_1 \in \mathbb{Z}$. Then $\sqrt[m]{N}$ is irrational.*

Proof. Suppose $\sqrt[m]{N}$ is rational. By the FTA, we may write $N = N_1^m N'$ for some $N_1, N' \in \mathbb{Z}_{>0}$, where N' is an integer not divisible by p^m for any prime p. Moreover, since N is not an m-th power, $N' \neq 1$. Thus there exists a prime number p such that $p \mid N'$ and $p^m \nmid N'$.

Suppose $\sqrt[m]{N}$ is rational. Then so is $\sqrt[m]{N'}$. Let $\sqrt[m]{N'} = a/b$ for some positive integers a, b. We may assume that $\gcd(a,b) = 1$. We have

$$N' b^m = a^m.$$

We have $p \mid N'$, hence $p \mid a^m = N' b^m$. It follows from Euclid's Theorem 1.11 that $p \mid a$, and hence $p^m \mid a^m$, i.e. $p^m \mid N' b^m$. Since $p^m \nmid N'$, in view of the FTA we now get $p \mid b^m$. This implies $p \mid b$, which contradicts the assumption that $\gcd(a,b) = 1$. □

Exercise 2.1. Which of the following numbers are irrational: $\sqrt{6}$, $\sqrt[3]{27}$, $\sqrt[4]{81}$, $\sqrt{20}$?

Exercise 2.2. Without referring to Proposition 2.3, prove that $\sqrt[3]{24}$ is irrational.

2.3 Euclid's proof of infinitude of primes

In your Discrete Math course you have seen the following:

Theorem 2.4. *There exist infinitely many prime numbers.*

The theorem is originally due to Euclid. We recall Euclid's proof here. Let $n \geq 1$. Suppose $p_1, \ldots, p_n$ are n distinct prime numbers. We show that there is a prime number other than $p_1, \ldots, p_n$. This will show that there are infinitely many primes.

Set

$$N = p_1 \cdots p_n + 1.$$

Then N (which is greater than 1) has a prime factorization. In particular, it has a prime divisor. Let q be a prime divisor of N. We claim that q is not any of the p_i. Indeed, if $q = p_i$ for some $1 \leq i \leq n$, then q divides both N and $N - 1 = p_1 \cdots p_n$, and hence q divides 1, which is absurd.

2.4 Euclid's proof of infinitude of primes revisited

Euclid's argument above actually gives us an upper bound on the n-th prime number. Indeed, for every positive integer n, let p_n be the n-th prime number. Euclid's argument tells us that

$$p_{n+1} \leq p_1 \cdots p_n + 1.$$

From this we can obtain an upper bound on the n-th prime and a lower bound on the prime counting function

$$\pi(x) := \text{the number of prime numbers} \leq x.$$

Proposition 2.5. (a) *Let p_n be the n-th prime number. Then*

$$p_n < 2^{2^n}.$$

(b) *For any $x \geq 2$,*

$$\pi(x) > \log\log(x).$$

Proof. (a) We argue by induction on n. We have $p_1 = 2 < 2^{2^1} = 4$. Suppose $p_i < 2^{2^i}$ for all $i \leq n$. Then by Euclid's argument,

$$p_{n+1} \leq p_1 \cdots p_n + 1 \leq (\prod_{i=1}^{n} 2^{2^i}) + 1 = 2^{\sum_{i=1}^{n} 2^i} + 1 = 2^{2^{n+1}-2} + 1 < 2^{2^{n+1}}.$$

(b) Let n be such that $p_n \leq x < p_{n+1}$, so that $\pi(x) = n$. By part (a), we have $p_{n+1} < 2^{2^{n+1}}$. Thus

$$\pi(x) + 1 = n + 1 > \log_2 \log_2 p_{n+1} > \log_2 \log_2 x,$$

so that

$$\pi(x) > \log_2 \log_2 x \ - 1.$$

This will give us the desired bound:

$$\pi(x) > \log_2 \log_2 x \ - 1 = \frac{\log\log x - \log\log 2}{\log 2} - 1 > \frac{\log\log x}{\log 2} - 1$$

$$= \log\log x + (\frac{1}{\log 2} - 1)\log\log x - 1 > \log\log x$$

if $x \geq e^{e^3}$. On the other hand, if $5 \leq x < e^{e^3}$, then $\log\log x < 3$ and $\pi(x) \geq 3 > \log\log x$. Finally, if $2 \leq x < 5$, then $\pi(x) \geq 1 > \log\log x$.

□

Note that the bound $\pi(x) > \log\log x$ is extremely bad (however, it is better than nothing)! For example,

$$\pi(1000) = 168, \qquad \log\log 1000 \sim 1.9$$
$$\pi(10^6) = 78498, \qquad \log\log(10^6) \sim 2.6.$$

Recall that by the prime number theorem (Theorem 2), $\pi(x)$ is asymptotic to $x/\log x$. Just for comparison, $10^6/\log(10^6)$ is roughly 72382.

2.5 Second proof of infinitude of primes and a better lower bound for $\pi(x)$

We now give a second proof of infinitude of primes, which will allow us to improve on Proposition 2.5.

Fix a positive integer j. Let $p_1, \ldots, p_j$ be the first j primes. For any x, let $N(x)$ be the number of positive integers $\leq x$ all whose prime divisors are $\leq p_j$. (To make the definition clear, note that $N(x)$ depends on the choice of our fixed j. For example, if $j = 3$, then $N(x)$ is the number of positive integers $\leq x$ all of whose prime divisors are among $2, 3, 5$ (the first $j = 3$ primes).)

We estimate $N(x)$ as follows. Given $n \leq x$, we can uniquely write n as

$$n = n_1^2 n',$$

where n' is squarefree. If all the prime divisors of n are $\leq p_j$, then $n' = p_1^{\alpha_1} \ldots p_j^{\alpha_j}$ with each exponent $\alpha_1, \ldots, \alpha_j$ either 0 or 1. Thus there are 2^j choices for n'. On the other hand, $n_1 \leq \sqrt{n} \leq \sqrt{x}$. Thus we obtain

$$N(x) \leq \sqrt{x}\, 2^j. \tag{2.1}$$

With the above background in mind, suppose there exist only finitely many primes. Take j to be the number of all primes. Then $N(x) = x$ for any positive integer x (since there are no primes other than $p_1, \ldots, p_j$!). Combing with (2.1) we get

$$x = N(x) \leq \sqrt{x}\, 2^j,$$

so that

$$\sqrt{x} \leq 2^j.$$

This is supposed to be true for every positive integer x, which is absurd.

In fact, the argument gives the following result:

Proposition 2.6. (a) *For any $x \geq 1$,*

$$\pi(x) \geq \frac{\log x}{\log 4}.$$

(b) *For any $n \geq 1$, denoting the n-th prime by p_n, we have*

$$p_n \leq 4^n.$$

Proof. (a) Given x, take $j = \pi(x)$ to define the function N as above. Then $N(x) = x$, as $p_1, \ldots, p_j$ are the only primes up to x. Equation (2.1) now gives

$$x = N(x) \leq \sqrt{x}\, 2^{\pi(x)},$$

so that

$$x \leq 4^{\pi(x)}. \tag{2.2}$$

Taking logarithms we obtain $\pi(x) \geq \frac{\log x}{\log 4}$, as desired.

(b) Given n, apply (2.2) with $x = p_n$ (so that $\pi(x) = n$). We get

$$p_n \leq 4^{\pi(x)} = 4^n.$$

□

Note that the estimate $\pi(x) \geq \log x / \log 4$ is still extremely poor (compare with the correct asymptotic of $x/\log(x)$ given by the prime number theorem), although it is an improvement on Proposition 2.5.

Exercise 2.3. Let n be an integer ≥ 2. Show that if n is not a prime number, then n has a divisor d with $1 < d \leq \sqrt{n}$.

2.6 Euler's proof of infinitude of primes

We now present[1] a third proof of infinitude of primes, due to Euler. The proof bridges number theory and analysis, and it is the birth of what we now call *analytic number theory*.

Suppose there are only finitely many primes. Let $p_1 < \cdots < p_n$ be all the primes. Then

$$\prod_{i=1}^{n} \frac{1}{1 - 1/p_i} \;=\; \prod_{i=1}^{n} (1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots) \;=\; \sum_{n=1}^{\infty} \frac{1}{n}\,, \tag{2.3}$$

where the first equality is by the formula for a geometric series and the second equality is by the fundamental theorem of arithmetic. (Every denominator n will appear exactly once as we expand the product.) This is absurd, since the right hand side (which is the harmonic series) diverges.

2.7 Primes in arithmetic progressions

By the division algorithm, every integer a is of one of the forms $4k$, $4k+1$, $4k+2$ and $4k+3$ for some $k \in \mathbb{Z}$. Those of the forms $4k$ and $4k+2$ are even and hence, except for the case $a = 2$, cannot be prime. The sequence of primes of the form $4k+1$ starts with

$$5, 13, 17, 29$$

[1] We skipped this section in class. You won't be tested on it.

and the sequence of primes of the form $4k+3$ starts with

$$3, 7, 11, 19.$$

We know there are infinitely many primes. Are there infinitely many primes of the form $4k+1$? Are there infinitely many primes of the form $4k+3$? The following adaptation of Euclid's argument answers the question in affirmative for primes of the latter form:

Proposition 2.7. *There are infinitely many primes of the form $4k+3$.*

Proof. Let $n \geq 1$ and $p_1, p_2, \ldots, p_n$ be primes of the form $4k+3$. We will show that there is a prime number q of the form $4k+3$ that is not equal to any of the p_i. This will show that there are infinitely many primes of the aforementioned form.

Let

$$N = 4p_1 \ldots p_n - 1.$$

Then N is also of the form $4k+3$. We claim that N must have a prime divisor of the form $4k+3$. Indeed, note that

$$(4k+1)(4k'+1) = 4(4kk' + k + k') + 1,$$

so that the product of a number of integers of the form $4k+1$ is of the same form. Since N is odd, it is a product of odd primes. If all the prime divisors of N were of the form $4k+1$, then N itself would also be of the form $4k+1$. But N is of the form $4k+3$, hence it must have a prime divisor of the form $4k+3$.

We are almost done. Let q be a prime divisor of N that is of the form $4k+3$. Then q is distinct from all of $p_1, \ldots, p_n$, for otherwise, $q \mid N$ and $q \mid N+1$ and hence $q \mid 1$, which is absurd. □

At this point of the course, we cannot prove that there are infinitely many primes of the form $4k+1$. We will come back to this in a few weeks.

Exercise 2.4. Show that there are infinitely many primes of the form $6k+5$.

More generally, fix an integer $b \geq 2$ (playing the role of the modulus). Every integer a is of the form

$$a = bk + r$$

for some r with $0 \leq r \leq b-1$. If r is such that $\gcd(b, r) > 1$, then $\gcd(b, r) \mid a$ and hence a cannot be prime unless $a = r$ is prime. So with the exception of finitely many primes (namely, possibly the primes $< b$), every prime number will be of one of the forms

$$bk + r, \quad (1 \leq r \leq b-1,\ \gcd(r, b) = 1).$$

Dirichlet was the first to prove that for each such choice of r, there are infinitely many primes of the form $bk + r$:

Theorem 2.8 (Dirichlet, 1837)**.** *Let b and r be integers and $\gcd(b, r) = 1$. Then there are infinitely many primes of the form $bk + r$.*

3 Week 3: Linear Diophantine equations, basics of congruence, and divisibility rules

3.1 Linear Diophantine equations

Proposition 3.1. *Let a, b be integers, not both zero. Let n be an integer. The equation*

$$ax + by = n$$

is soluble in $\mathbb{Z}$ (i.e., there exist integers x, y satisfying the equation) if and only if $\gcd(a, b)$ divides n.

Proof. Let $d = \gcd(a, b)$.

$\Rightarrow$: If $ax + by = n$ for some $x, y \in \mathbb{Z}$, then by Proposition 1.2(d) the facts that $d \mid a$ and $d \mid b$ imply $d \mid ax + by = n$.

$\Leftarrow$: Suppose $d \mid n$. By Proposition 1.9, there exist integers x', y' such that $ax' + by' = d$. Multiplying by n/d (which is an integer because $d \mid n$) we get

$$a\,(x' \cdot \frac{n}{d}) \;+\; b\,(y' \cdot \frac{n}{d}) \;=\; n.$$

□

Example 3.2. The equation $6x - 9y = 10$ is not soluble in $\mathbb{Z}$ because $\gcd(6, 9) = 3 \nmid 10$. But the equation $6x - 9y = 12$ is soluble in $\mathbb{Z}$ because $3 \mid 12$. For every integer n, the equation $12x + 17y = n$ has solutions in $\mathbb{Z}$ since $\gcd(12, 17) = 1 \mid n$.

Next, we discuss how to find all the integral (or integer) solutions to $ax + by = n$ when the equation has solutions. This has two steps. Suppose $d = \gcd(a, b)$ and $d \mid n$ (so that the equation is soluble in $\mathbb{Z}$). In the first step, we find one solution to $ax + by = n$. This can be done either by (i) inspection (when possible), or (ii) using the Euclidean algorithm to first find a solution to $ax' + by' = d$ and then multiplying by n/d to get a solution to $ax + by = n$.

Having found one solution, we now discuss how to find the general solution. First note that the two equations

$$ax + by = n \quad \text{and} \quad (a/d)\,x \;+ (b/d)\,y \;= n/d$$

have the exact same set of solutions. So we may replace the equation on the left by the one on the right. Since $\gcd(a/d, b/d) = 1$, we may focus on equations where the coefficients of x and y are relatively prime.

Proposition 3.3. *Let $\gcd(a, b) = 1$ and $(x, y) = (x_0, y_0)$ be one integral solution to*

$$ax + by = n.$$

Then the general solution to the equation is of the form

$$x = x_0 - kb, \quad y = y_0 + ka \qquad (k \in \mathbb{Z}). \tag{3.1}$$

Proof. First, note that any x, y as above are indeed integers and satisfy the equation:

$$a(x_0 - kb) + b(y_0 + ka) = ax_0 + by_0 - kab + kab = ax_0 + by_0 = n.$$

It remains to show that every solution is of the form (3.1) for some integer k. Let x, y be integers satisfying $ax + by = n$. Then

$$a(x - x_0) + b(y - y_0) = (ax + by) - (ax_0 + by_0) = n - n = 0.$$

It follows that

$$a\,(x - x_0) = -b\,(y - y_0).$$

Suppose $a \neq 0$ (the case $b \neq 0$ is similar). Since a divides $b(y - y_0)$ and $\gcd(a, b) = 1$, it follows from Exercise 1.5 that a divides $y - y_0$. So $y - y_0 = ka$ for some $k \in \mathbb{Z}$. We thus have

$$a(x - x_0) = -bka.$$

Dividing by a we get $x - x_0 = -kb$. Thus $y = y_0 + ka$ and $x = x_0 - kb$, as desired. □

Example 3.4. Find all integral solutions to

$$6x - 9y = 12.$$

Solution. We have $\gcd(6, -9) = 3 \mid 12$, thus the equation is soluble in $\mathbb{Z}$. To give the solutions, let us first divide the equation by $\gcd(6, -9) = 3$ to obtain the equivalent equation (i.e., with the same set of solutions)

$$2x - 3y = 4.$$

By inspection, $(x_0, y_0) = (2, 0)$ is a solution. Applying Proposition 3.3 to the equation $2x - 3y = 4$, the general solution is given by

$$x = 2 + 3k, \quad y = 0 + 2k = 2k \qquad (k \in \mathbb{Z}).$$

□

Example 3.5. Find all integers x, y such that

$$899x - 851y = 3,$$

if such integers exist.

Solution. Let us first find $\gcd(899, 851)$:

$$899 = 851 \cdot 1 + 48; \quad 851 = 48 \cdot 17 + 35; \quad 48 = 35 \cdot 1 + 13$$
$$35 = 13 \cdot 2 + 9; \quad 13 = 9 \cdot 1 + 4; \quad 9 = 4 \cdot 2 + 1; \quad 4 = 1 \cdot 4 + 0.$$

So $\gcd(899, 851) = 1$ and the equation $899x - 851y = 3$ is soluble in $\mathbb{Z}$. To find one solution, first we use our previous computations of the Euclidean algorithm to find a solution to $899x - 851y = 1$:

$$1 = 9 - 4 \cdot 2 = 9 \cdot 3 - 13 \cdot 2 = 35 \cdot 3 - 13 \cdot 8 = -48 \cdot 8 + 35 \cdot 11 = 851 \cdot 11 - 48 \cdot 195 = -899 \cdot 195 + 851 \cdot 206.$$

Thus

$$x_0 = 3 \cdot (-195) = -585, \quad y_0 = 3 \cdot (-206) = -618$$

is a solution to $899x - 851y = 3$. Since $\gcd(899, 851) = 1$, the general solution to this equation is now given by

$$x = -585 + 851k, \quad y = -618 + 899k \qquad (k \in \mathbb{Z}).$$

□

Example 3.6. A bank machine can dispense \$20 and \$50 bills. Euclid is trying to withdraw \$350 using this bank machine. Find all the possible combinations of bills that he may get.

Solution. We are interested in the solutions to

$$20x + 50y = 350$$

in the *non-negative* integers. Dividing the equation by $\gcd(20, 50) = 10$ we obtain the equivalent equation

$$2x + 5y = 35.$$

One solution to this is $(x_0, y_0) = (0, 7)$. The general solution in the integers is given by

$$x = -5k, \quad y = 7 + 2k \qquad (k \in \mathbb{Z}).$$

We are only interested in the solutions where both x and y are ≥ 0. These will be obtained for $k = 0, -1, -2, -3$. The possibilities are

$$(x, y) \in \{(0, 7),\ (5, 5),\ (10, 3),\ (15, 1)\}.$$

□

So far, we have discussed linear Diophantine equations in two variables. The picture generalizes to a higher number of variables. For instance, one has:

Proposition 3.7. *Let a, b, c be integers, not all zero. Then for every integer n, the equation*

$$ax + by + cz = n$$

is soluble in $\mathbb{Z}$ if and only if $\gcd(a, b, c)$ divides n.

Here, $\gcd(a, b, c)$ is the greatest common divisor of a, b, c, defined in the obvious way. For example, $\gcd(6, 10, 15) = 1$.

3.2 Congruence: Definition and basic properties

You have seen the following definition in your Discrete Math course:

Definition 3.8 (Congruence)**.** Fix $m \in \mathbb{Z}$. We say an integer a is congruent to an integer b mod m and write $a \equiv b \pmod{m}$ if $m \mid a - b$.

For example, $1 \equiv 5 \pmod{4}$.

Lemma 3.9. *Let $m \in \mathbb{Z}$. Then*

(a) *(Reflexivity) For every $a \in \mathbb{Z}$, we have $a \equiv a \pmod{m}$.*

(b) *(Symmetry) For every $a, b \in \mathbb{Z}$, if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.*

(c) *(Transitivity) For every $a, b, c \in \mathbb{Z}$, if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.*

Proof. (a) $a - a = 0$ and $m \mid 0$.

(b)

$$a \equiv b \pmod{m} \iff m \mid a - b \overset{\text{Prop. 1.2(c)}}{\iff} m \mid b - a \iff b \equiv a \pmod{m}$$

(c) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $m \mid a - b$ and $m \mid b - c$, hence

$$m \mid (a - b) + (b - c) = a - c,$$

i.e., $a \equiv c \pmod{m}$.

□

On recalling the notion of an equivalence relation (see your Discrete Math notes), the previous lemma asserts the following:

Corollary 3.10. *For every $m \in \mathbb{Z}$, congruence mod m is an equivalence relation on $\mathbb{Z}$.*

Definition 3.11. The equivalence classes of (the equivalence relation) congruence mod m are called congruence classes or residue classes mod m.

There are exactly m congruence classes mod m, namely, the classes of $0, \ldots, m - 1$.

Proposition 3.12. *Let $m, d \in \mathbb{Z}$ and $d \mid m$. Then*

$$a \equiv b \pmod{m} \quad \Rightarrow \quad a \equiv b \pmod{d}.$$

Proof. Suppose $a \equiv b \pmod{m}$. Then $m \mid a - b$ and $d \mid m$, hence $d \mid a - b$. □

For example, if $a \equiv b \pmod{6}$, then a and b are also congruent mod 3.

Proposition 3.13. *Let $m \in \mathbb{Z}$. Suppose*

$$\begin{aligned} a &\equiv b \pmod{m} \\ c &\equiv d \pmod{m}. \end{aligned} \tag{3.2}$$

Then

$$a + c \equiv b + d \pmod{m} \tag{3.3}$$

$$ac \equiv bd \pmod{m}. \tag{3.4}$$

Proof. (3.3) is clear: since $m \mid a - b$ and $m \mid c - d$, we have

$$m \mid (a - b) + (c - d) = (a + c) - (b + d),$$

therefore (3.3) holds.

To see (3.4), note that

$$ac - bd = ac - bd + ad - ad = a(c - d) + d(a - b).$$

By (3.2), m divides $a - b$ and $c - d$, hence m divides the right hand side of the above equation and therefore its left hand side. □

Corollary 3.14. *Let $m \in \mathbb{Z}$. Suppose*

$$a \equiv b \pmod{m}.$$

Then we have:

(a) $ka \equiv kb \pmod{m}$ *for every* $k \in \mathbb{Z}$

(b) $a^n \equiv b^n \pmod{m}$ *for every* $n \in \mathbb{Z}_{\geq 0}$

(c) *For every polynomial $f(x)$ with coefficients in $\mathbb{Z}$, we have*

$$f(a) \equiv f(b) \pmod{m}.$$

Proof. All of these follow directly from Proposition 3.13.

(a) This is the special case of (3.4) with $c = d = k$.

(b) The case $n = 0$ is trivial. Now argue by induction on n: if $a^n \equiv b^n \pmod{m}$ for some $n \geq 0$, combining with $a \equiv b \pmod{m}$, in view of Proposition 3.13 we get $a^{n+1} \equiv b^{n+1} \pmod{m}$.

(c) This follows from the previous two parts and the additivity property in Proposition 3.13: Write $f(x) = \sum_{n \geq 0} c_n x^n$. Then by part (b), we have $a^n \equiv b^n \pmod{m}$ for every integer $n \geq 0$. Now by part (a) we get $c_n a^n \equiv c_n b^n \pmod{m}$ for every integer $n \geq 0$. Finally, now by the additivity property in Proposition 3.13 we get

$$\sum_{n \geq 0} c_n a^n \equiv \sum_{n \geq 0} c_n b^n \pmod{m}.$$

□

Example 3.15. What is the last (= the rightmost) digit of 291^{2026}?

Solution. Since $291 \equiv 1 \pmod{10}$, by Corollary 3.14 (b) we have

$$291^{2026} \equiv 1^{2026} \equiv 1 \pmod{10}.$$

Thus the last digit of 291^{2026} is 1. □

Example 3.16. Find the last digit of 2^{102}.

We will give two solutions.

First solution. Let us calculate the first few powers of 2 mod 10 and see if we can observe any patterns:

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 6, \quad 2^5 \equiv 2 \cdot 6 \equiv 2,$$

where all the congruences are mod 10. We notice a pattern: We have $2^5 \equiv 2^1 \pmod{10}$. Multiplying by 2 (using Proposition 3.14(a) with $k = 2$) we get $2^6 \equiv 2^2 \pmod{1}0$, and then

multiplying by 2 again we get $2^7 \equiv 2^3 \pmod{10}$, and so on. By induction we can see that for any $n \in \mathbb{Z}_{>0}$,

$$2^n \equiv \begin{cases} 2 \pmod{10} & \text{if } n \equiv 1 \pmod 4 \\ 4 \pmod{10} & \text{if } n \equiv 2 \pmod 4 \\ 8 \pmod{10} & \text{if } n \equiv 3 \pmod 4 \\ 6 \pmod{10} & \text{if } n \equiv 0 \pmod 4. \end{cases}$$

In particular, since $102 \equiv 2 \pmod 4$, we have

$$2^{102} \equiv 4 \pmod{10}.$$

□

Second solution. We have $2^2 \equiv 4 \pmod{10}$. Squaring both sides

$$2^4 \equiv 4^2 \equiv 6 \pmod{10}.$$

By successive squaring,

$$\begin{aligned} 2^8 &\equiv 6^2 \equiv 6 \pmod{10} \\ 2^{16} &\equiv 6 \pmod{10} \\ 2^{32} &\equiv 6 \pmod{10} \\ 2^{64} &\equiv 6 \pmod{10} \end{aligned}$$

(where we used the fact that $6^2 \equiv 6 \pmod{10}$ in every step). Since

$$102 = 64 + 32 + 4 + 2,$$

we have

$$2^{102} = 2^{64}2^{32}2^4 2^2 \equiv 6 \cdot 6 \cdot 6 \cdot 4 \overset{\text{why?}}{\equiv} 6 \cdot 4 \equiv 4 \pmod{10}.$$

The last digit of 2^{102} is thus 4. □

Example 3.17. We have $1 \equiv 6 \pmod 5$. By Corollary 3.14, we have

$$\begin{aligned} 6^{100} - 2 \cdot 6^{50} + 4 &\equiv 1^{100} - 2 \cdot 1^{50} + 4 \pmod 5 \\ &\equiv 1 - 2 + 4 \equiv 3 \pmod 5. \end{aligned}$$

(Our first congruence reads $f(1) \equiv f(6) \pmod 5$ for $f(x) = x^{100} - 2x^{50} + 4$.)

3.3 Application: Divisibility rules

As an application of the basic properties of congruence, here we establish some well-known divisibility "rules" in terms of the decimal representations of integers. Most of these rules are familiar to you but some may be new.

Proposition 3.18 (Some divisibility rules)**.** *Let n be a positive integer with decimal representation $a_k \cdots a_1 a_0$ (with $a_j \in \{0, 1, \ldots, 9\}$ for each j).*

(a) *(divisibility by 2) n is divisible by 2 if and only if a_0 is one of 0,2,4,6,8.*

(b) *(divisibility by 3) We have*

$$n \equiv \sum_{j=0}^{k} a_j \pmod 3.$$

In particular, n is divisible by 3 if and only if the sum of the digits of n is divisible by 3.

(c) *(divisibility by 4) n is congruent mod 4 to the integer with decimal representation a_1a_0 (i.e., consisting of the last two digits) mod 4.*

(d) *(divisibility by 5) We have*

$$n \equiv a_0 \pmod 5.$$

In particular, n is divisible by 5 if and only if a_0 is 0 or 5.

(e) *(divisibility by 9) We have*

$$n \equiv \sum_{j=0}^{k} a_j \pmod 9.$$

In particular, n is divisible by 9 if and only if the sum of the digits of n is divisible by 9.

(f) *(divisibility by 10) The remainder of n in division by 10 is a_0.*

(g) *(divisibility by 11) We have*

$$n \equiv a_0 - a_1 + a_2 - a_3 + \cdots \pmod{11}.$$

In particular, n is divisible by 11 if and only if the alternating sum of the digits of n is divisible by 11.

Proof. We will only discuss the proofs of the divisibility rules mod 3,9 and 11, leaving the rest as exercises.

Divisibility by 9 and 3: We have

$$n = \sum_{j\geq 0} 10^j\, a_j.$$

Since $10 \equiv 1 \pmod 9$, by Corollary 3.14 we have

$$n \equiv \sum_{j\geq 0} 10^j\, a_j \equiv \sum_{j\geq 0} 1^j\, a_j \equiv \sum_{j\geq 0} 1 \cdot a_j \equiv \sum_{j\geq 0} a_j \pmod 9.$$

This gives the assertions in part (e). Moreover, in view of Proposition 3.12, we also get the same congruences mod 3 and hence the assertions in part (b).

Divisibility by 11: We have $10 \equiv -1 \pmod{11}$. Thus

$$n \equiv \sum_{j\geq 0} 10^j\, a_j \equiv \sum_{j\geq 0} (-1)^j\, a_j \pmod{11}.$$

□

Example 3.19. We have

$$123456 \equiv 6 - 5 + 4 - 3 + 2 - 1 \equiv 3 \pmod{11}.$$

Exercise 3.1. Let k be a positive integer such that $3 \mid k$. Show that $10^k \equiv 1 \pmod{37}$. (Hint: Factor 999. What is 1000 mod 37?)

Exercise 3.2. Suppose

$$a \equiv b \pmod{m}.$$

Show that $\gcd(a, m) = \gcd(b, m)$.

Exercise 3.3. Let a, b, c, m be integers and $a \neq 0$. Show that

$$b \equiv c \pmod{m} \iff ab \equiv ac \pmod{am}.$$

4 Week 4: Congruence equations, units, and the Chinese remainder theorem

4.1 Cancellation property for congruences

Recall from Corollary 3.14 that if $b \equiv c \pmod{m}$, then $ab \equiv ac \pmod{m}$. In general, the converse is not true. For instance,

$$2 \cdot 3 \equiv 2 \cdot 0 \pmod{6}$$

but $3 \not\equiv 0 \pmod{6}$. However, we have the following important property:

Proposition 4.1. *If*

$$ab \equiv ac \pmod{m},$$

then

$$b \equiv c \pmod{m/\gcd(a, m)}.$$

Proof. Suppose $ab \equiv ac \pmod{m}$. Then

$$m \mid ab - ac = a(b - c). \tag{4.1}$$

Let $d = \gcd(a, m)$. Write $a = da'$ and $m = dm'$, so that $\gcd(a', m') = 1$. It follows from (4.1) that

$$m' \mid a'(b - c).$$

Since $\gcd(a', m') = 1$, from this we get $m' \mid b - c$. Thus $b \equiv c \pmod{m'}$, as desired. □

For example, if $2b \equiv 2c \pmod{6}$, then $b \equiv c \pmod{3}$.
The proposition immediate gives the following important result:

Corollary 4.2. *If* $ab \equiv ac \pmod{m}$ *and* $\gcd(a, m) = 1$, *then* $b \equiv c \pmod{m}$.

For example,

$$2a \equiv 2b \pmod{11} \implies a \equiv b \pmod{11}$$

because 2 and 11 are relatively prime.

4.2 What is a congruence equation?

Example 4.3. Is there any integer x such that

$$2x^2 \equiv 2 \pmod 6? \tag{4.2}$$

By Corollary 3.14, if $x = x_0$ is one integral solution to this equation, then any integer of the form $x \equiv x_0 \pmod 6$ is a solution. Thus solutions to (4.2) are congruence classes mod 6. Every integer is congruent to exactly one of the numbers

$$0, 1, 2, 3, 4, 5$$

mod 6. By inspection, we see that $x = 1, 2, 4, 5$ satisfy (4.2). Thus the general solution to (4.2) is

$$x \equiv 1, 2, 4, 5 \pmod 6$$

(or equivalently, $x \equiv \pm 1, \pm 2 \pmod 6$). Note that (4.2) has four solutions mod 6.

Equation (4.2) is an example of a congruence equation. More generally, a congruence equation is an equation of the form

$$f(x) \equiv n \pmod m,$$

where n and m are integers, and f is a polynomial with integer coefficients. All of n, m, f are given and the unknown is x. The solutions to this equation will be none, one, or more congruence classes mod m.

Congruence equations can be useful for studying Diophantine equations too:

Example 4.4. Show that the equation

$$x^2 - 3z^2 = 2$$

has no solutions in $\mathbb{Z}$.

Proof. Suppose there exist integers x, y satisfying the equation. Then

$$x^2 \equiv 2 \pmod 3$$

(we say we *reduced the equation mod 3*). But this congruence has no solution: Any integer x is congruent to one of $0, \pm 1$ mod 3, and none of these satisfies $x^2 \equiv 2 \pmod 3$. Thus there is no integer x satisfying $x^2 \equiv 2 \pmod 3$. □

4.3 Linear congruences

Linear congruences are the simplest type of congruence equations. They are equations of the form $ax \equiv n \pmod m$.

Proposition 4.5. *Let a, n, m be integers and $m \geq 2$. Let $d = \gcd(a, m)$.*

(a) The equation

$$ax \equiv n \pmod m$$

is soluble (i.e., has solutions in $\mathbb{Z}$) if and only if $d \mid n$.

(b) Suppose $d = 1$. The the equation $ax \equiv n \pmod{m}$ has a unique solution mod m.

Proof. (a) By definition of congruence, the equation $ax \equiv n \pmod{m}$ is soluble in $\mathbb{Z}$ if and only if there exist integers x, y such that $ax + my = n$. By Proposition 3.3, such x, y exist if and only if $d \mid n$.

(b) By the previous part, the equation $ax \equiv n \pmod{m}$ is soluble. We need to show that its solution is unique mod m. For this, suppose x_1 and x_2 are two solutions to the equation. Then

$$ax_1 \equiv ax_2 \pmod{m}.$$

By assumption, a and m are relatively prime. It follows from Corollary 4.2 that $x_1 \equiv x_2 \pmod{m}$, as desired. □

Example 4.6. Consider the congruence equation

$$6x \equiv 9 \pmod{33}.$$

Since $\gcd(6, 33) = 3$ divides 9, the equation is soluble. To find its solutions, first note that by Exercise 3.3, the equation is equivalent to the congruence equation

$$2x \equiv 3 \pmod{11}. \tag{4.3}$$

Since $\gcd(2, 11) = 1$, the latter equation has a unique solution mod 11. By inspection, we see that $x = 7$ is a solution, and hence the general solution is

$$x \equiv 7 \pmod{11}.$$

If we want to express the solutions in terms of congruence classes mod 33, the answer is

$$x \equiv 7 + 11k \pmod{33},$$

which gives three different congruence classes

$$x \equiv 7, 18, 29 \pmod{33}.$$

Exercise 4.1. Let $d = \gcd(a, m)$. Suppose $d \mid n$. Show that the linear congruence

$$ax \equiv n \pmod{m}$$

has exactly d solutions mod m. (Hint: Consider the equation $(a/d)x \equiv n/d \pmod{m/d}$ first.)

4.4 Multiplicative inverses and units mod m

Definition 4.7 (Units and inverses mod m)**.** Let m be an integer ≥ 2. An integer a is called a unit mod m if there exists an integer b such that $ab \equiv 1 \pmod{m}$. An integer b with this property is called a multiplicative inverse (or for simplicity, an inverse) of a mod m.

Let m be an integer ≥ 2. It is clear from the definition that if a is a unit mod m with a (multiplicative) inverse b, then b is also a unit mod m with an inverse a.

Given an integer a, by Proposition 4.5(a) the equation

$$ax \equiv 1 \pmod{m}$$

is soluble if and only if $\gcd(a, m) = 1$. Moreover, if $\gcd(a, m) = 1$, then by Proposition 4.5(b), the equation has a unique solution mod m. In conclusion, a is a unit mod m if and only if $\gcd(a, m) = 1$, and moreover, the inverse of a unit a mod m is unique mod m. The inverse of a mod m is usually denoted by $a^{-1} \pmod{m}$.

4.5 Finding multiplicative inverses

Let a be a unit mod m. Then to find the multiplicative inverse of a mod m we need to find the solution to the equation

$$ax \equiv 1 \pmod{m}$$

(which is unique mod m). This can be done sometimes through inspection. More systematically, it can be done by using the Euclidean algorithm to find integers x, y such that

$$ax + my = 1.$$

Example 4.8. Is 4 a unit mod 17? If it is, find its inverse.

Proof. The number 4 is indeed a unit mod 17 because $\gcd(4, 17) = 1$. To find the inverse, we need to find x such that

$$4x \equiv 1 \pmod{17}.$$

Note that from the general theory we know that the equation has a unique solution mod 17. By inspection, we see that

$$4 \times 13 = 52 \equiv 1 \pmod{17}.$$

Thus the multiplicative inverse of 4 mod 17 is 13. (Here is one way to inspect: Go through positive numbers that are 1 mod 17: $1, 18, 35, 52$, etc. We see that $52 = 4 \cdot 13$.)

Alternatively, we could approach the problem more systematically by finding a solution to $4x + 17y = 1$ using the Euclidean algorithm. Leaving the computations as an exercise, we get that

$$x = -4,\ y = 1$$

is a solution. Thus $x = -4$ is a solution to $4x \equiv 1 \pmod{17}$ (and it is the unique solution mod 17 to this congruence). Thus the multiplicative inverse of 4 mod 17 is -4. (Note that $13 \equiv -4 \pmod{17}$, so this is consistent with our earlier conclusion.) □

Example 4.9. Solve the congruence

$$4x \equiv 2 \pmod{17}.$$

Solution. Since $\gcd(4, 17) = 1$, the equation has a unique solution mod 17. To find this solution, we may multiply both sides with $4^{-1} \pmod{17}$, which we found in the previous example to be 13:

$$x \equiv 2 \cdot 4^{-1} \equiv 2 \cdot 13 \equiv 26 \equiv 9 \pmod{17}.$$ □

Example 4.10. Solve the congruence

$$6x \equiv 9 \pmod{33}.$$

Solution. Since $\gcd(6, 33) = 3 \mid 9$, the equation is soluble. To solve the equation, first divide by $\gcd(6, 33)$ to obtain the equivalent equation

$$2x \equiv 3 \pmod{11}.$$

Now 2 is a unit mod 11 with multiplicative inverse 6. Multiplying the equation by 6 we get

$$x \equiv 3 \cdot 6 \equiv 18 \equiv 7 \pmod{11}.$$ □

4.6 Systems of linear congruences and the Chinese remainder theorem

So far we have considered a single congruence equation. We will now consider systems of congruence equations. The key result is the following:

Theorem 4.11 (The Chinese remainder theorem)**.** *Let $m_1, m_2, \ldots, m_k$ be pairwise coprime positive integers. Let $r_1, r_2, \ldots, r_k$ be integers. Then the system of equations*

$$\begin{aligned} x &\equiv r_1 \pmod{m_1} \\ x &\equiv r_2 \pmod{m_2} \\ &\vdots \\ x &\equiv r_k \pmod{m_k} \end{aligned} \tag{4.4}$$

has a unique solution mod $M = \prod_{i=1}^{k} m_i$.

Proof. There are two assertions: that a solution exists, and that it is unique (i.e., there are no two different solutions) mod M. We first prove the latter.

Uniqueness: Suppose $x = x_1$ and $x = x_2$ both satisfy the equations. Then

$$x_1 \equiv x_2 \pmod{m_i}$$

for $i = 1, \ldots, k$. That is, $m_i \mid x_1 - x_2$ for $i = 1, \ldots, k$. Since the m_i are pairwise coprime, it follows that $M \mid x_1 - x_2$. (The assumption of pairwise coprimality is crucial here.) Thus $x_1 \equiv x_2 \pmod{M}$.

Existence: We will show this by constructing a solution. For each $i = 1, \ldots, k$, let $M_i = M/m_i$ (= the product of all our moduli with m_i dropped from the product). Since $m_1, \ldots, m_k$ are pairwise coprime, we have $\gcd(M_i, m_i) = 1$, so that M_i is a unit mod m_i. Let n_i be a solution to $M_i n_i \equiv 1 \pmod{m_i}$. Set

$$x = \sum_{i=1}^{k} M_i n_i r_i.$$

We claim that x satisfies the system of equations (4.4). Indeed, fix j with $1 \leq j \leq k$. Then for every $i \neq j$, it follows from the definition of M_i that $m_j \mid M_i$. Thus

$$x \;=\; \sum_{i=1}^{k} M_i n_i r_i \;\equiv\; M_j n_j r_j \;\equiv\; 1 \cdot r_j \;\equiv\; r_j \pmod{m_j}. \qquad \square$$

Example 4.12. Find all x such that

$$\begin{aligned} x &\equiv 7 \pmod{12} \\ x &\equiv 3 \pmod{5}. \end{aligned} \tag{4.5}$$

Solution. Since 12 and 5 are coprime, by the Chinese remainder theorem the equation has a unique solution mod $12 \cdot 5 = 60$. To find the solution, we follow the procedure given in the

proof of the existence assertion of the Chinese remainder theorem. Following the notation therein, set $m_1 = 12$, $m_2 = 5$, $r_1 = 7$, and $r_2 = 3$. Then $M = m_1 m_2 = 60$. We have $M_1 = m_2 = 5$ and $M_2 = m_1 = 12$. Next, we find an inverse of M_i mod m_i for $i = 1, 2$:

$$\begin{aligned} \overbrace{5}^{M_1} n_1 &\equiv 1 \pmod{\overbrace{12}^{m_1}} \\ \underbrace{12}_{M_2} n_2 &\equiv 1 \pmod{\underbrace{5}_{m_2}}. \end{aligned}$$

We see $n_1 = 5$ and $n_2 = 3$ satisfy these. A solution to (4.5) is

$$x = M_1 n_1 r_1 + M_2 n_2 r_2 = 5 \cdot 5 \cdot 7 + 12 \cdot 3 \cdot 3 = 283.$$

By the Chinese remainder theorem, the general solution to (4.5) is

$$x \equiv 283 \equiv 43 \pmod{60}. \qquad \square$$

Example 4.13. Find all x such that

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 1 \pmod 7. \end{aligned} \tag{4.6}$$

Solution. The moduli 3,5,7 are pairwise coprime, so by the Chinese remainder theorem, the equation has a unique solution mod $3 \cdot 5 \cdot 7 = 105$. To find it, following the notation of the proof of Theorem 4.11, set $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, $r_1 = 2$, $r_2 = 3$, $r_3 = 1$. Then $M = 105$, $M_1 = m_2 m_3 = 35$, $M_2 = m_1 m_3 = 21$, $M_3 = m_1 m_2 = 15$. Next, for each i we need an inverse n_i of M_i mod m_i:

$$\begin{aligned} \overbrace{35}^{M_1} n_1 \equiv 1 \pmod{\overbrace{3}^{m_1}} &\iff 2n_1 \equiv 1 \pmod 3 \iff n_1 \equiv 2 \pmod 3 \\ 21\, n_2 \equiv 1 \pmod 5 &\iff n_2 \equiv 1 \pmod 5 \\ 15\, n_3 \equiv 1 \pmod 7 &\iff n_3 \equiv 1 \pmod 7 \end{aligned}$$

We may take $n_1 = -1$, $n_2 = 1$, $n_3 = 1$. Then a solution to (4.6) is

$$x = M_1 n_1 r_1 + M_2 n_2 r_2 + M_3 n_3 r_3 = 35 \cdot (-1) \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 1 = 8.$$

The general solution to (4.6) is

$$x \equiv 8 \pmod{105}. \qquad \square$$

5 Week 5: Chinese remainder theorem continued and residue classes

5.1 The Chinese remainder theorem continued

Example 5.1 (When the coefficients of x may not be 1)**.** Find all x such that

$$\begin{aligned} 2x &\equiv 4 \pmod 8 \\ x &\equiv 1 \pmod 3 \\ 3x &\equiv 2 \pmod 5. \end{aligned} \tag{5.1}$$

Solution. Here we are not quite in the setting of the Chinese remainder theorem, since some of the coefficients of x are not 1. Here, the first step will be to find an equivalent system of equations that fits the setting of the Chinese remainder theorem. The first equation $2x \equiv 4 \pmod 8$ is equivalent to $x \equiv 2 \pmod 4$ (by Corollary 4.2). The third equation $3x \equiv 2 \pmod 5$ is equivalent to $x \equiv 4 \pmod 5$ (obtained by multiplying with $2 = 3^{-1} \pmod 5$). Thus the system of equations (5.1) is equivalent to

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 1 \pmod 3 \\ x &\equiv 4 \pmod 5. \end{aligned} \tag{5.2}$$

This system is in the setting of the Chinese remainder theorem (note that the moduli are also pairwise coprime). It has a unique solution mod $4 \cdot 3 \cdot 5 = 60$. Following the notation used earlier we have

$$m_1 = 4,\ m_2 = 3,\ m_3 = 5,\ M = 60,\ M_1 = 15,\ M_2 = 20,\ M_3 = 12,\ r_1 = 2,\ r_2 = 1,\ r_3 = 4.$$

For an inverse of $M_1 = 15 \bmod m_1 = 4$ we may take $n_1 = 3$. For an inverse of $M_2 = 20 \bmod m_2 = 3$ we may take $n_2 = 2$. For an inverse of $M_3 = 12 \bmod m_3 = 5$ we may take $n_3 = -2$. A solution to (5.2) is

$$x = M_1 n_1 r_1 + M_2 n_2 r_2 + M_3 n_3 r_3 = 15 \cdot 3 \cdot 2 + 20 \cdot 2 \cdot 1 + 12 \cdot (-2) \cdot 4 = 34.$$

The general solution to (5.2) (equivalently, (5.1)) is $x \equiv 34 \pmod{60}$. □

Example 5.2 (When the moduli are not coprime)**.** Find all x such that

$$\begin{aligned} x &\equiv -6 \pmod{20} \\ x &\equiv 4 \pmod{15} \\ x &\equiv 1 \pmod 3. \end{aligned} \tag{5.3}$$

Solution. Here we are not in the setting of the Chinese remainder theorem because the moduli are not pairwise coprime. We can deal with this by decomposing the interfering moduli into distinct prime powers, as follows.

By the Chinese remainder theorem (see Remark 5.4 below),

$$x \equiv -6 \pmod{20} \iff \begin{cases} x \equiv -6 \pmod 4 \\ x \equiv -6 \pmod 5 \end{cases} \iff \begin{cases} x \equiv 2 \pmod 4 \\ x \equiv 4 \pmod 5. \end{cases}$$

On the other hand,

$$x \equiv 4 \pmod{15} \iff \begin{cases} x \equiv 4 \equiv 1 \pmod 3 \\ x \equiv 4 \pmod 5. \end{cases}$$

It follows that the system (5.3) is equivalent to the system of congruences

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 1 \pmod 3. \end{aligned}$$

This is exactly the system (5.2) that we solved on Example 5.1. The general solution is $x \equiv 34 \pmod{60}$. □

Example 5.3 (When the moduli are not coprime)**.** Find all x such that

$$\begin{aligned} x &\equiv 4 \pmod{20} \\ x &\equiv 3 \pmod{24}. \end{aligned} \tag{5.4}$$

Solution. Again we first we try to rewrite the system in a way that the moduli are pairwise coprime. We have

$$x \equiv 4 \pmod{20} \iff \begin{cases} x \equiv 4 \equiv 0 \pmod{4} \\ x \equiv 4 \pmod{5} \end{cases}$$

and

$$x \equiv 3 \pmod{24} \iff \begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 3 \pmod{3}. \end{cases}$$

We observe that the two equations $x \equiv 4 \pmod{20}$ and $x \equiv 3 \pmod{24}$ are not compatible: the first equation would imply that $x \equiv 0 \pmod{4}$, while the second equation implies that $x \equiv 3 \pmod{8}$ and hence $x \equiv 3 \pmod{4}$. Thus the system of congruences (5.4) has no solutions. □

REMARK 5.4. Let $m_1, \dots m_k \in \mathbb{Z}$ be pairwise coprime and $a \in \mathbb{Z}$. Then for every integer x,

$$x \equiv a \pmod{\prod_{i=1}^{k} m_i} \quad \text{if and only if} \quad \begin{cases} x \equiv a \pmod{m_1} \\ x \equiv a \pmod{m_2} \\ \quad \vdots \\ x \equiv a \pmod{m_k}. \end{cases}$$

Indeed, from left to right this follows from Proposition 3.12. From right to left this is by the uniqueness part of the Chinese remainder theorem: $x = a$ is clearly a solution to the system on the right, and hence any solution to the system satisfies $x \equiv a \pmod{m_1 \cdots m_k}$.

In particular, if $M = p_1^{\alpha_1} \cdots, p_k^{\alpha_k}$ with $p_1, \dots, p_k$ distinct primes, then $x \equiv a \pmod{M}$ if and only if $x \equiv a \pmod{p_i^{\alpha_i}}$ for $i = 1, \dots, k$.

5.2 Residue classes

Before reading this section, review the part of your Discrete Math course on equivalence relations.

Fix a positive integer m. By Lemma 3.9, congruence mod m is a reflexive, symmetric, and transitive relation on $\mathbb{Z}$. This makes congruence mod m an equivalence relation on $\mathbb{Z}$. The equivalence classes of this relation are called *residue classes* or *congruence classes* mod m. For any integer a, the residue class of a mod m denoted by $[a]_m$ is

$$[a]_m = \{x \in \mathbb{Z} \,|\, x \equiv a \pmod{m}\} = \{a + km \,|\, k \in \mathbb{Z}\}.$$

For every integer b,

$$a \equiv b \pmod{m} \iff [a]_m = [b]_m.$$

Residue classes mod m provide a partition of $\mathbb{Z}$. Each of the numbers in a residue class is called a representative of that residue class.

By the division algorithm, every integer a is congruent mod m to exactly one of $0, 1, \ldots, m-1$. Thus there are exactly m residue classes mod m, namely,

$$[0]_m\,,\ [1]_m\,,\ \ldots\,,\ [m-1]_m.$$

Moreover, by Proposition 3.13, the notions of units and inverses mod m descend to residue classes. That is, we may talk about when a residue class is a unit, and if so what its inverse is.

Example 5.5. Take the modulus to be $m = 4$. There are 4 residue classes mod 4, namely:

$$\begin{aligned}
\{\ldots\,,-8\,,-4\,,0\,,4\,,8\,,\ldots\} &= [-4] = [0] = [4] = \cdots\\
\{\ldots\,,-7\,,-3\,,1\,,5\,,9\,,\ldots\} &= [-7] = [1] = [5] = \cdots\\
\{\ldots\,,-6\,,-2\,,2\,,6\,,10\,,\ldots\} &= [2] = [6] = [10] = \cdots\\
\{\ldots\,,-5\,,-1\,,3\,,7\,,11\,,\ldots\} &= [3] = [-1] = [7] = \cdots\,,
\end{aligned}$$

where for simplicity, we wrote $[\ ]$ instead of $[\ ]_4$. The residue classes $[1]$ and $[3]$ are the units (i.e., those with multiplicative inverses), and $[1]^{-1} = [1]$ and $[3]^{-1} = [3]$.

From now on, when the modulus m is clear from the context (which will be often the case for us), we will simply write $[a]$ instead of $[a]_m$.

6 Week 6: Complete sets of residues mod m, Euler's φ function, Fermat's and Euler's theorems

6.1 Complete sets of residues mod m, coprime to m, and Euler's function

Definition 6.1 (A complete set of residues mod m)**.** Let m be a positive integer. A complete set of residues mod m is a set of integers that contains exactly one element from each residue class mod m.

For example,

$$\{0, 1, 2, 3\}$$

and

$$\{4, 6, 7, -3\}$$

are two examples of complete sets of residues mod 4. Every complete set of residues mod m has m elements.

Definition 6.2. We say a residue class $[a]_m$ is coprime (or relatively prime) to m if $\gcd(a, m) = 1$.

Note that the above definition makes sense because of Exercise 3.2.

Definition 6.3 (A complete set of residues coprime to m)**.** A complete set of residues coprime to m is a set consisting of exactly one element from each residue class coprime to m.

For example, the residue classes coprime to 6 are $[1]$ and $[5]$. A complete set of residues coprime to 6 is $\{1, 5\}$. Another complete set of residues coprime to 6 is $\{7, 11\}$.

Definition 6.4 (Euler's φ function)**.** For every positive integer m, set $\varphi(m)$ to be the number of residue classes coprime to m. Equivalently, $\varphi(m)$ is the number of elements of any complete set of residues coprime to m.

Since the integers a with $1 \leq a \leq m$ form a complete set of residues mod m, the numbers a with $1 \leq a \leq m$ and $\gcd(a, m) = 1$ form a complete set of residues coprime to m. Thus

$$\varphi(m) = |\{a \in \mathbb{Z} \,|\, 1 \leq a \leq m,\, \gcd(a, m) = 1\}. \tag{6.1}$$

The function φ was first defined by Euler and for this reason is known as Euler's function. It is sometimes also called Euler's *totient* function. It is one of the most basic functions in number theory.

For example, the numbers $1 \leq a \leq 12$ relatively prime to 12 are $1, 5, 7, 11$. Hence $\varphi(12) = 4$. Similarly we can check that

$$\varphi(1) = 1,\ \varphi(2) = 1,\ \varphi(4) = 2,\ \varphi(11) = 10.$$

Note that for any prime p, $\varphi(p) = p - 1$, since every positive integer $< p$ is coprime to p.

Remark 6.5. (a) A collection of integers S is a complete set of residues mod m if and only if $|S| = m$ and no two elements of S are congruent mod m.

(b) A collection of integers S is a complete set of residues coprime to m if and only if $|S| = \varphi(m)$, every element of S is coprime to m, and no two elements of S are congruent mod m.

We close this subsection with the following useful result.

Proposition 6.6. *Let* $\gcd(a, m) = 1$.

(a) *Let $r_1, \ldots, r_m$ be a complete set of residues mod m. Then $ar_1, \ldots ar_m$ is also a complete set of residues mod m.*

(b) *Let $r_1, \ldots, r_{\varphi(m)}$ be a complete set of residues coprime to m. Then $ar_1, \ldots, ar_{\varphi(m)}$ is also a complete set of residues coprime to m.*

Proof. (a) Since $\gcd(a, m) = 1$ and $r_1, \ldots, r_m$ are pairwise incongruent mod m, by Corollary 4.2, the numbers $ar_1, \ldots ar_m$ are also pairwise incongruent mod m. The claim follows, because $ar_1, \ldots ar_m$ are m numbers belonging to different residue classes mod m (hence we must have exactly one number from each residue class).

(b) Since $\gcd(a, m) = 1$ and $r_1, \ldots, r_{\varphi(m)}$ are pairwise incongruent mod m, so are the numbers $ar_1, \ldots, ar_{\varphi(m)}$. Moreover, for each i, by assumption we have $\gcd(r_i, m) = 1$. Putting together with $\gcd(a, m) = 1$ we obtain that $\gcd(ar_i, m) = 1$. Thus $ar_1, \ldots, ar_{\varphi(m)}$ is a collection of $\varphi(m)$ numbers that are coprime to m and pairwise incongruent mod m. The claim follows.

□

6.2 How to compute $\varphi(m)$

The function φ has the following key property:

Theorem 6.7. *Let m, n be coprime positive integers. Than*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

We will prove this in the next subsection, taking it for granted for the rest of this subsection. In general, a function $f : \mathbb{Z}_{>0} \to \mathbb{R}$ with the property that for every positive integers m, n,

$$\gcd(m, n) = 1 \quad \Longrightarrow \quad f(mn) = f(m)f(n)$$

is called a *multiplicative* function. Thus Theorem 6.7 asserts that φ is multiplicative. Note that if f is a multiplicative function, by induction on k we obtain

$$\text{if } m_1, \ldots, m_k \text{ pairwise coprime, then } f(m_1 m_2 \cdots m_k) = f(m_1)f(m_2)\cdots f(m_k).$$

Let $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $p_1, \ldots, p_k$ are distinct primes. Thanks to the multiplicativity of φ (and since the $p_i^{\alpha_i}$ are pairwise coprime), we have

$$\varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}).$$

Thus the question of computing $\varphi(m)$ is reduced to computing each $\varphi(p_i^{\alpha_i})$. The latter task is easy:

Lemma 6.8. *Let p be a prime number. Then for every $\alpha \in \mathbb{Z}_{>0}$,*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1).$$

Proof. We have

$$\varphi(p^\alpha) \;=\; |\{1 \le a \le p^\alpha : \gcd(a, p^\alpha) = 1\}| \;=\; p^\alpha - |\{1 \le a \le p^\alpha : \gcd(a, p^\alpha) > 1\}|.$$

For every a, we have $\gcd(a, p^\alpha) > 1$ if and only if $p \mid a$ (because the only prime divisor of p^α is p). It follows that

$$\varphi(p^\alpha) = p^\alpha - \left| \{1 \le a \le p^\alpha : p \mid a\} \right| = p^\alpha - p^\alpha/p,$$

which gives the claimed formulas. □

Putting together Theorem 6.7 and Lemma 6.8, we obtain:

Corollary 6.9. *Let $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $p_1, \ldots, p_k$ are distinct primes and $\alpha_1, \ldots, \alpha_k \ge 1$. Then*

$$\varphi(m) \;=\; \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) \;=\; \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1).$$

Example 6.10. Calculate $\varphi(1000)$.

Solution. We have $1000 = 2^3 \times 5^3$. Thus

$$\varphi(1000) = \varphi(2^3)\varphi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 4 \cdot 100 = 400.$$

□

Example 6.11. Calculate $\varphi(900)$.

Solution. We have $900 = 2^2 3^2 5^2$. Thus

$$\varphi(900) = \varphi(2^2)\varphi(3^2)\varphi(5^2) = (2^2 - 2^1)(3^2 - 3)(5^2 - 5) = 2 \cdot 6 \cdot 20 = 240.$$

□

Exercise 6.1. True or false: If $m \geq 2$ is a power of 2, then $\varphi(m) = m/2$.

REMARK 6.12. Let $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $p_1, \ldots, p_k$ are distinct primes and $\alpha_1, \ldots, \alpha_k \geq 1$. We may rewrite the formula for $\varphi(m)$ as follows:

$$\varphi(m) \;=\; \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = \prod_{i=1}^{k} p_i^{\alpha_i}(\frac{p_i - 1}{p_i}) \;=\; (\prod_{i=1}^{k} p_i^{\alpha_i})\,(\prod_{i=1}^{k} \frac{p_i - 1}{p_i}) \;=\; m \prod_{i=1}^{k}(1 - \frac{1}{p_i}).$$

We record the conclusion: for any positive integer m, we have

$$\varphi(m) = m \cdot \prod_{p|m} (1 - \frac{1}{p}). \tag{6.2}$$

Here, the product is over all prime divisors of m.

Exercise 6.2. Show that $\varphi(m) = m/3$ if and only if $m = 2^\alpha 3^\beta$ for some positive integers α, β. (Hint: Use the formula (6.2).)

Exercise 6.3. Let $f : \mathbb{Z}_{>0} \to \mathbb{R}$ be a multiplicative function. Define the function $g : \mathbb{Z}_{>0} \to \mathbb{R}$ by

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

where the sum is over all the positive divisors d of m. Show that g is also multiplicative.

6.3 Proof of multiplicativity of φ

Our goal in subsection is to prove Theorem 6.7. To get there, we need a lemma:

Lemma 6.13. *Let m and n be coprime positive integers. Let $\{a_1, \ldots, a_m\}$ be a complete set of residues mod m, and $\{b_1, \ldots, b_n\}$ be a complete set of residues mod n. Then the numbers $na_i + mb_j$ ($1 \leq i \leq m$ and $1 \leq j \leq n$) form a complete set of residues mod mn.*

Before the proof, let us look at an example:

Example 6.14. The set $\{0,1\}$ and $\{1,2,3\}$ are respectively complete sets of residues mod 2 and mod 3. Since 2 and 3 are coprime, Part (a) of Lemma 6.13 asserts that the numbers $3a+2b$ with $a \in \{0,1\}$ and $b \in \{1,2,3\}$ form a complete set of residues mod $2 \times 3 = 6$. These numbers are

$$2, 4, 6, 5, 7, 9.$$

Proof of Lemma 6.13. It suffices to show that no two of the numbers $na_i + mb_j$ are congruent mod mn, as then we have mn numbers belonging to distinct residue classes mod mn, which hence must form a complete set of residues mod mn.

Suppose

$$na_i + mb_j \equiv na_{i'} + mb_{j'} \pmod{mn} \tag{6.3}$$

for some $1 \leq i, i' \leq m$ and $1 \leq j, j' \leq n$. By Proposition 3.12, we may reduce the congruence mod m. We get

$$na_i \equiv na_{i'} \pmod{m}$$

(the terms mb_j and $mb_{j'}$ are zero mod m). Since n and m are relatively prime, by Corollary 4.2 we get

$$a_i \equiv a_{i'} \pmod{m}.$$

Since $a_1, \ldots, a_m$ form a complete set of residues mod m, we get $i = i'$. Similarly, reducing (6.3) mod n we will see that $j = j'$. □

Suppose m and n are coprime integers and $\{a_1, \ldots, a_m\}$ (resp. $\{b_1, \ldots, b_n\}$) is a complete set of residues mod m (resp. mod n). By the last lemma, the mn numbers $a_i n + b_j m$ form a complete set of residues mod mn. To count $\varphi(mn)$, we may thus go through the numbers $a_i n + b_j m$ and count the ones that are coprime to mn. The following lemma will help us do this.

Lemma 6.15. *Let* $\gcd(m,n) = 1$. *Then for every integers* a, b, *we have*

$$\gcd(an + bm, mn) = 1 \quad \Longleftrightarrow \quad \gcd(a,m) = \gcd(b,n) = 1.$$

Proof. We have

$$\begin{aligned} \gcd(an+bm, mn) = 1 &\overset{(1)}{\Longleftrightarrow} \gcd(an+bm, m) = 1 \text{ and } \gcd(an+bm, n) = 1 \\ &\overset{(2)}{\Longleftrightarrow} \gcd(an, m) = 1 \text{ and } \gcd(bm, n) = 1 \\ &\overset{(3)}{\Longleftrightarrow} \gcd(a, m) = 1 \text{ and } \gcd(b, n) = 1. \end{aligned}$$

Here, (1) is by Exercise 1.9, (2) uses Lemma 1.7 and (3) is because of the key assumption that $\gcd(m,n) = 1$. □

We are ready to prove Theorem 6.7:

Proof of Theorem 6.7. Let m and n be coprime positive integers. Let $S(m)$ be a complete set of residues mod m and $S(n)$ a complete set of residues mod n. By Lemma 6.13, the set

$$\{an + bm : a \in S(m), b \in S(n)\}$$

is a complete set of residues mod mn. Moreover, by Lemma 6.15, $an + bm$ is coprime to mn if and only if $\gcd(a, m) = 1$ and $\gcd(b, n) = 1$. Thus

$$\begin{aligned}\varphi(mn) &= |\{an + bm : a \in S(m), b \in S(n), \gcd(an + bm, mn) = 1\}| \\ &= |\{an + bm : a \in S(m), b \in S(n), \gcd(a, m) = \gcd(b, n) = 1\}| \\ &= \varphi(m)\varphi(n).\end{aligned}$$

□

In fact, we obtain the following:

Corollary 6.16. *Let $m, n \in \mathbb{Z}_{>0}$ be coprime. Let $a_1, \ldots, a_{\varphi(m)}$ (resp. $b_1, \ldots, b_{\varphi(n)}$) form a complete set of residues coprime to m (resp. n). Then the numbers $a_i n + b_j m$ with $1 \leq i \leq \varphi(m)$ and $1 \leq j \leq \varphi(n)$ form a complete set of residues coprime to mn.*

Proof. First, by the proof of Lemma 6.13, the numbers $a_i n + b_j m$ with $1 \leq i \leq \varphi(m)$ and $1 \leq j \leq \varphi(n)$ are pairwise incongruent mod mn. Moreover, by Lemma 6.15, each $a_i n + b_j m$ is coprime to mn. Thus the $a_i n + b_j m$ with i, j as above form a set of $\varphi(m)\varphi(n)$ numbers, all of which are coprime to mn, and no two of which are congruent mod mn. Since $\varphi(mn) = \varphi(m)\varphi(n)$, these numbers form a complete set of residues coprime to mn. □

6.4 Euler's and Fermat's theorems

We are ready to establish the following important result.

Theorem 6.17 (Euler's theorem)**.** *Let $m \in \mathbb{Z}_>0$ and $a \in \mathbb{Z}$. Suppose a and m are coprime. Then*

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

Proof. Let $r_1, \ldots, r_{\varphi(m)}$ form a complete set of residues coprime to m. Since $\gcd(a, m) = 1$, by Proposition 6.6(b), $ar_1, \ldots, ar_{\varphi(m)}$ also form a complete set of residues coprime to m. In particular, $ar_1, \ldots, ar_{\varphi(m)}$ are merely a rearrangement of $r_1, \ldots, r_{\varphi(m)}$ *mod* m. Thus

$$\prod_{i=1}^{\varphi(m)} r_i \equiv \prod_{i=1}^{\varphi(m)} ar_i \pmod{m}.$$

Factoring the a's out in the second product we get

$$\prod_{i=1}^{\varphi(m)} r_i \equiv a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} r_i \pmod{m}. \tag{6.4}$$

We are almost done: Since each r_i is coprime to m, the product $\prod_{i=1}^{\varphi(m)} r_i$ is also coprime to m. Thus (6.4) implies

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

□

The special case where m is a prime number was known before Euler:

Corollary 6.18 (Fermat's ("little") theorem)**.** *Let p be a prime number. Let $a \in \mathbb{Z}$ with $p \nmid a$. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. Take $m = p$ in Euler's theorem. The condition $\gcd(a, p) = 1$ is equivalent to $p \nmid a$. Moreover, we have $\varphi(p) = p - 1$ since p is prime. Euler's theorem gives us the desired congruence. □

Example 6.19. (1) Since 7 is prime and $7 \nmid 2$, by Fermat's (or Euler's) theorem we have

$$2^6 \equiv 1 \pmod{7}.$$

Note that $2^6 = 64$ is indeed congruent to 1 mod 7.

(2) Let us take $m = 100$ and $a = 3$. We have

$$\varphi(100) = \varphi(4)\varphi(25) = (4 - 2) \cdot (25 - 5) = 40.$$

Since $\gcd(100, 3) = 1$, Euler's theorem tells us

$$3^{40} \equiv 1 \pmod{100}.$$

Thus the last two digits of 3^{40} are 01.

REMARK 6.20. Suppose $\gcd(a, m) = 1$, so that by Euler's theorem $a^{\varphi(m)} \equiv 1 \pmod{m}$. If $k \equiv k' \pmod{\varphi(m)}$ for integers $k' \geq k \geq 0$, then we have

$$a^{k'} = a^{k'-k}a^k = (a^{\varphi(m)})^{(k-k')/\varphi(m)}a^k \overset{\text{Euler's theorem}}{\equiv} 1^{(k-k')/\varphi(m)}a^k \equiv a^k \pmod{m}.$$

We record the conclusion:

$$\textit{If } \gcd(a, m) = 1 \textit{ and } k' \equiv k \pmod{\varphi(m)}, \textit{ then } a^{k'} \equiv a^k \pmod{m}.$$

Example 6.21. Let us try to calculate $24^{100} \pmod{17}$. Since 17 is prime and $17 \nmid 24$, by Fermat's theorem

$$24^{16} \equiv 1 \pmod{17}.$$

Since $100 \equiv 4 \pmod{\varphi(17) = 16}$, by Fermat's theorem and Remark 6.20 we have

$$24^{100} \overset{\text{mod } 17}{\equiv} 24^4 \equiv 7^4 \pmod{17}.$$

To calculate 7^4 mod 17, we note that

$$7^4 = 49^2 \overset{\text{why?}}{\equiv} (-2)^2 \equiv 4 \pmod{17}.$$

Thus $24^{100} \equiv 4 \pmod{17}$.

Example 6.22. Let us calculate

$$3^{49} \pmod{50}.$$

First note that $50 = 2 \cdot 5^2$. In particular, since 50 is not prime, we are not in the situation of Fermat's theorem. We have

$$\varphi(50) = \varphi(2)\varphi(25) = 20.$$

Since $\gcd(3, 50) = 1$, by Euler's theorem we have

$$3^{20} \equiv 1 \pmod{50}.$$

Since $49 \equiv 9 \pmod{\varphi(50) = 20}$, we have

$$3^{49} \overset{\text{mod } 50}{\equiv} 3^9 \equiv (3^4)^2 \cdot 3 \overset{\text{why?}}{\equiv} 31^2 \cdot 3 \overset{\text{why?}}{\equiv} 11 \cdot 3 \equiv 33 \pmod{50}.$$

Example 6.23 (with $\gcd(a, m) > 1$)**.** Let us calculate

$$14^{2020} \pmod{100}.$$

Note that since 14 and 100 are not coprime, we are not in the setting of Euler's theorem. Since $100 = 4 \times 25$ and $\gcd(4, 25) = 1$, by the Chinese remainder theorem, the congruence class of any number (in particular, 14^{2020}) mod 100 is determined by its congruence classes mod 4 and mod 25. We compute 14^{2020} mod 4 and mod 25 separately first. Since $2 \mid 14$, we have $2^{2020} \mid 14^{2020}$, and thus $4 \mid 14^{2020}$. That is,

$$14^{2020} \equiv 0 \pmod{4}. \tag{6.5}$$

Moving on to calculating 14^{2020} mod 25, since $\gcd(14, 25) = 1$ and $\varphi(25) = 20 \mid 2020$, by Euler's theorem we have

$$14^{2020} \equiv 1 \pmod{25}. \tag{6.6}$$

From (6.5) and (6.6), 14^{2020} is a solution to the system of equations

$$\begin{aligned} x &\equiv 0 \pmod{4} \\ x &\equiv 1 \pmod{25}. \end{aligned}$$

By the Chinese remainder theorem (Theorem 4.11), this system has a unique solution mod 100. By inspection (or alternatively, following the approach given earlier in the proof of the Chinese remainder theorem) we see that $x = 76$ is a solution. It follows that

$$14^{2020} \equiv 76 \pmod{100}.$$

Exercise 6.4. Calculate $6^{2026} \pmod{25}$.

Exercise 6.5. Calculate $4^{201} \pmod{600}$. (Final answer: $304 \pmod{600}$)

7 Week 7: Order mod m, Wilson's theorem, quadratic residues

7.1 Order mod m

Definition 7.1 (Order mod m)**.** Let m be a positive integer. For any integer a coprime to m, we define the order of a mod m to be the smallest $d \in \mathbb{Z}_{>0}$ with the property that $a^d \equiv 1 \pmod{m}$.

Let $\gcd(a, m) = 1$. Then by Euler's theorem, $a^{\varphi(m)} \equiv 1 \pmod{m}$. Thus the order of a mod m exists and is $\leq \varphi(m)$. In fact, we can say more:

Proposition 7.2. *Let $m \in \mathbb{Z}_{>0}$, $a \in \mathbb{Z}$, and $\gcd(a, m) = 1$. Let d be the order of a mod m.*

(a) For every $k \in \mathbb{Z}_{\geq 0}$, we have

$$a^k \equiv 1 \pmod{m} \iff d \mid k.$$

(b) We have $d \mid \varphi(m)$

(c) For every $k, k' \in \mathbb{Z}_{\geq 0}$, we have

$$a^{k'} \equiv a^k \pmod{m} \iff k' \equiv k \pmod{d}.$$

(d) The numbers $1, a, a^2, \ldots, a^{d-1}$ are distinct (i.e., pairwise incongruent) mod m.

Proof. (a) Given $k \in \mathbb{Z}_{\geq 0}$, by the division algorithm ("dividing k by d") we can write $k = qd + r$ for some integers q, r with $0 \leq r < d$. By the definition of order, we have $a^d \equiv 1 \pmod{m}$, so that

$$a^k = a^{qd+r} = (a^d)^q a^r \equiv 1^q a^r \equiv a^r \pmod{m}. \tag{7.1}$$

Since $r \in \{0, 1, \ldots, d-1\}$, it follows from the minimality property of d (i.e., that d is the *smallest* positive integer such that $a^d \equiv 1 \pmod{m}$) that $a^r \equiv 1 \pmod{m}$ if and only if $r = 0$. The result follows:

$$a^k \equiv 1 \pmod{m} \overset{(7.1)}{\iff} a^r \equiv 1 \pmod{m} \iff r = 0 \iff d \mid k.$$

(b) By Euler's theorem, $a^{\varphi(m)} \equiv 1 \pmod{m}$. Thus by part (a) we have $d \mid \varphi(m)$.

(c) We may assume $k' \geq k$. Since $\gcd(a, m) = 1$ (which implies $\gcd(a^{k'-k}, m) = 1$), by the cancellation property $a^{k'} \equiv a^k \pmod{m}$ is equivalent to $a^{k'-k} \equiv 1 \pmod{m}$. By part (a), the latter is equivalent to $d \mid k' - k$.

(d) This is immediate from part (c).

□

Example 7.3. Let d be the order of 3 mod 40 (note that $\gcd(3, 40) = 1$). Since $\varphi(40) = 16$, we know by Proposition 7.2(b) that $d \mid 16$. To find d, let us consider powers of 3 mod 40:

$$3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^3 \equiv 27,\ 3^4 \equiv 81 \equiv 1,$$

where all congruences are mod 40.[2] It follows that $d = 4$. Note that this indeed divides 16, as we already knew from the last proposition. For any integer k, we have

$$3^k \equiv 1 \pmod{40} \iff 4 \mid k$$

(see Proposition 7.2(a)). More generally, for any k', k, we have

$$3^{k'} \equiv 3^k \pmod{40} \iff 4 \mid k' - k.$$

The numbers $1, 3, 3^2, 3^{d-1} = 3^3$ are distinct mod 40. (See Parts (c) and (d) of Proposition 7.2.)

7.2 Wilson's theorem

In this subsection we will prove the following result:

Theorem 7.4 (Wilson's theorem)**.** *Let p be an odd prime number. Then*

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

Thus for example, $16! \equiv -1 \pmod{17}$.

The proof will use the following lemma, which is important in its own right:

Lemma 7.5. *Let p be a prime number and $x \in \mathbb{Z}$. Then*

$$x^2 \equiv 1 \pmod{p} \iff x \equiv \pm 1 \pmod{p}.$$

That is, the only solutions to $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1 \pmod{p}$. Note that if p is an odd prime, these 1 and -1 are different mod p and hence $x^2 \equiv 1 \pmod{p}$ has exactly two solutions mod p.

Proof of Lemma 7.5. The implication $\Leftarrow$ is trivial so we only need to establish $\Rightarrow$. Suppose $x^2 \equiv 1 \pmod{p}$. Then

$$p \mid x^2 - 1 = (x-1)(x+1).$$

Since p is prime, it follows that p divides $x - 1$ or $x + 1$. That is, x is congruent to 1 or -1 mod p. □

Remark 7.6. Let p be an odd prime number. By the last lemma, there are exactly two residue classes mod p that are their own inverses mod p. These are the residue classes of 1 and -1.

Remark 7.7. For an arbitrary integer m, the equation $x^2 \equiv 1 \pmod{m}$ may have more than two solutions mod m. For instance, $x^2 \equiv 1 \pmod{8}$ has four solutions $x \equiv 1, 3, 5, 7 \pmod{8}$.

We can now prove Wilson's theorem:

[2] In fact, we didn't have to compute 3^3 since we know d divides 16 and hence, $d \neq 3$.

Proof of Theorem 7.4. The set $S = \{1, 2, \ldots, p-1\}$ is a complete set of residues coprime to p. Each element of S has a unique inverse mod p in S. By Lemma 7.5, the only elements that are their own inverses are $1, p-1$. Thus $S \setminus \{1, p-1\}$ can be partitioned into $(p-3)/2$ inverse pairs mod p. Thus

$$\prod_{i=1}^{p-1} i \;\equiv\; 1 \cdot 1^{(p-3)/2} \cdot (p-1) \;\equiv\; -1 \pmod{p}.$$

(The first congruence is because $S \setminus \{1, p-1\}$ can be partitioned into inverse pairs mod p, and each inverse pair multiplies out to give 1.) □

7.3 Quadratic residues: The statement of the problem and the definitions

Our next topic is on congruence equations of the form

$$x^2 \equiv a \pmod{m}. \tag{7.2}$$

Here, a and m are given. Note that the equation depends on the residue class of a mod m (rather than the integer a). Also, its solutions, if they exist, will be some residue classes mod m.

The Chinese remainder theorem reduces the equation to the case where the modulus is a prime power, as illustrated by the example below.

Example 7.8. [3] Consider the equation

$$x^2 \equiv 1 \pmod{72}. \tag{7.3}$$

Since $72 = 8 \cdot 9$, by the Chinese remainder theorem we have

$$x^2 \equiv 1 \pmod{72} \quad \Longleftrightarrow \quad \begin{cases} x^2 \equiv 1 \pmod{8} \\ x^2 \equiv 1 \pmod{9}. \end{cases}$$

Both $x^2 \equiv 1 \pmod 8$ and $x^2 \equiv 1 \pmod 9$ are soluble. In fact, direct computations show that

$$\begin{aligned} x^2 \equiv 1 \pmod{8} \quad &\Longleftrightarrow \quad x \equiv \pm 1, \pm 3 \pmod{8} \\ x^2 \equiv 1 \pmod{9} \quad &\Longleftrightarrow \quad x \equiv \pm 1 \pmod{9}. \end{aligned}$$

Thus

$$x^2 \equiv 1 \pmod{72} \quad \Longleftrightarrow \quad \begin{cases} x \equiv \pm 1, \pm 3 \pmod{8} \\ x \equiv \pm 1 \pmod{9}. \end{cases}$$

By the Chinese remainder theorem, each choice for $([x]_8, [x]_9)$ gives exactly one residue class mod 72. Thus there are 8 solutions to (7.3) mod 72:

$$x^2 \equiv 1 \pmod{72} \quad \Longleftrightarrow \quad x \equiv \pm 1, \pm 17, \pm 19, \pm 35 \pmod{72}.$$

Back to the general equation (7.2), thanks to the Chinese remainder theorem we thus may assume that the modulus m is a prime power. In fact, it turns out that the core case is the case where m is an odd prime. The problem we will consider is the following:

[3] We skipped this example in class.

Problem 7.9. Let p be an odd prime number. Given an integer a, determine if the equation

$$x^2 \equiv a \pmod{p}$$

is soluble. (That is, determine if a has a square root mod p.)

Note that this problem focuses on whether a solution exist. It does not ask to *find* the solutions (if they exist). Also, whether or not $x^2 \equiv a \pmod{p}$ is soluble depends on the residue class of a mod p (rather that the integer a).

The case $a = 0$ (or $a \equiv 0 \pmod{p}$) of the last problem is easy: $x^2 \equiv 0 \pmod{p}$ is soluble, and its only solution is $x \equiv 0 \pmod{p}$. We thus may focus on the case where $p \nmid a$.

Definition 7.10 (Quadratic residues)**.** Let p be an odd prime number and a an integer with $p \nmid a$. We say a is a quadratic residue mod p if there exists $x \in \mathbb{Z}$ such that

$$x^2 \equiv a \pmod{p}.$$

We say a is a quadratic non-residue if there is no such x.

If $a \equiv b \pmod{p}$, the equations $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ are equivalent. Thus whether or not a is a quadratic residue mod p depends on the residue class of a mod p. We say $[a]_p$ is a quadratic residue (resp. non-residue) class if a is a quadratic residue (resp. non-residue). A set of integers consisting of exactly one number from each quadratic residue (resp. non-residue) class mod p is called a complete set of quadratic residues (resp. non-residues) mod p.

Example 7.11. Let us find the quadratic residues mod $p = 5$. The numbers $\pm 1, \pm 2$ form a complete set of residues coprime to 5. We have $(\pm 1)^2 \equiv 1$ and $(\pm 2)^2 \equiv 4 \pmod{5}$. Thus the the quadratic residue classes mod 5 are classes of 1 and 4. The numbers 1,4 form a complete set of quadratic residues mod 5. The quadratic non-residue classes are classes of 2,3. We see that out of the 4 residue classes coprime to 5, half are quadratic and half are not quadratic.

Example 7.12. Let us find the quadratic residues mod $p = 11$. The numbers $\pm 1, \pm 2, \pm 3, \pm 4, \pm 5$ form a complete set of residues coprime to 11. We have

$$(\pm 1)^2 \equiv 1, \quad (\pm 2)^2 \equiv 4, \quad (\pm 3)^2 \equiv 9, \quad (\pm 4)^2 \equiv 16 \equiv 5, \quad (\pm 5)^2 \equiv 25 \equiv 3,$$

where all congruences are mod 11. Thus the quadratic residue classes mod 11 are classes of $1, 4, 9, 5, 3$ (and these numbers form a complete set of quadratic residues mod 11). The remaining classes, i.e., the classes of $2, 6, 7, 8, 10$ are quadratic non-residues. Notice that in this example too, exactly half of the residue classes coprime to 11 are quadratic and half are not quadratic. We shall see soon that in fact, for every odd prime p, there are exactly $(p-1)/2$ quadratic residue classes and $(p-1)/2$ quadratic non-residue classes.

The following notation is very useful:

Definition 7.13 (The Legendre symbol)**.** Let p be an odd prime, $a \in \mathbb{Z}$ and $p \nmid a$. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

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

Example 7.14. The equation $x^2 \equiv 2 \pmod 3$ is not soluble because ± 1 form a complete set of residues coprime to 3 and neither is a solution to $x^2 \equiv 2 \pmod 3$. Thus

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

On the other hand, $x^2 \equiv 5 \pmod{11}$ is soluble (see Example 7.12). Thus

$$\left(\frac{5}{11}\right) = 1.$$

Note that the $x^2 \equiv 5 \pmod{11}$ has exactly two solutions mod 11 (see Example 7.12).

The Legendre symbol $\left(\frac{a}{p}\right)$ is only defined if p is an odd prime and $p \nmid a$.

Remark 7.15. If $a \equiv b \pmod p$, then the two equations $x^2 \equiv a \pmod p$ and $x^2 \equiv b \pmod p$ are equivalent. By the definition of the Legendre symbol, we thus have

$$a \equiv b \pmod p \quad \Longrightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Remark 7.16. Suppose that $a \in \mathbb{Z}$ is a perfect square, i.e., there exists an integer b such that $b^2 = a$. Then for every odd prime p with $p \nmid a$ we have

$$\left(\frac{a}{p}\right) = 1,$$

as the equation $x^2 \equiv a \pmod p$ has a solution $x = b$. For example, for every odd prime p,

$$\left(\frac{1}{p}\right) = \left(\frac{4}{p}\right) = 1.$$

Our goal for the next few lectures is to solve Problem 7.9, which amounts to computing the Legendre symbol $\left(\frac{a}{p}\right)$.

7.4 Quadratic residues: The statements of the main results

In this subsection we will state without proof the main results that will allow us to solve Problem 7.9. The theorems are due to Gauss. The proofs will be given later.

The first result is the following:

Theorem 7.17 (Multiplicativity of the Legendre symbol)**.** *Let p be an odd prime number. Suppose $a, b \in \mathbb{Z}$ and $p \nmid ab$. Then*

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

The second result, which is the main theorem of the theory of quadratic residues, is the following:

Theorem 7.18. *(a) (The quadratic reciprocity) Suppose p and q are two distinct odd prime numbers. Then*

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

(b) Let p be an odd prime number. Then

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

and

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

The quadratic reciprocity (Theorem 7.18(a)) is arguably the deepest result we will see in this course. This remarkable result, together with the determination of $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ given in Theorem 7.18(b) (which are sometimes called the supplements to the quadratic reciprocity), Theorem 7.17 and Remark 7.15 provide a powerful machinery to compute the Legendre symbol, as we will see in the examples in the next subsection.

7.5 Quadratic residues: Examples

In this subsection we will take Theorems 7.17 and 7.18 for granted and give several examples.

Example 7.19. Since $13 \equiv 1 \pmod 4$, by Theorem 7.18(b), -1 is a quadratic residue mod 13. In other words, the equation $x^2 \equiv -1 \pmod{13}$ has a solution. On the other hand, since $11 \equiv 3 \pmod 4$, -1 is not a quadratic residue mod 11 and the equation $x^2 \equiv -1 \pmod{11}$ has no solutions.

Example 7.20. By Theorem 7.18(b), 2 is a quadratic residue mod the primes 17 and 31, because 17 and 31 are respectively congruent to 1 and -1 mod 8. On the other hand, 2 is not a quadratic residue mod 13 or 19 because these primes are congruent to ± 3 mod 8.

Example 7.21. Calculate the Legendre symbol $\left(\frac{3}{71}\right)$. Does the equation $x^2 \equiv 3 \pmod{71}$ have any solutions?

Solution. Note that both 3 and 71 are prime. Since they are both congruent to 3 mod 4, by quadratic reciprocity we have

$$\left(\frac{3}{71}\right) = -\left(\frac{71}{3}\right). \tag{7.4}$$

Since $71 \equiv 2 \pmod 3$, by Remark 7.15 we have

$$\left(\frac{71}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

where the last equation is because 2 is not a quadratic residue mod 3 (as the only quadratic residue class mod 3 is the class of $(\pm 1)^2 \equiv 1 \pmod 3$). Substituting in (7.4) we get

$$\left(\frac{3}{71}\right) = -(-1) = 1.$$

Thus 3 is a quadratic residue mod 71, or in other words, the equation $x^2 \equiv 3 \pmod{71}$ has a solution. □

Example 7.22. Determine if the equation

$$x^2 \equiv 35 \pmod{103}$$

has any solutions.

Solution. Note that 103 is prime. We will calculate the Legendre symbol

$$\left(\frac{35}{103}\right).$$

We have

$$\begin{aligned}\left(\frac{35}{103}\right) = \left(\frac{5\cdot 7}{103}\right) &\overset{\text{Thm 7.17}}{=} \left(\frac{5}{103}\right)\left(\frac{7}{103}\right)\\ &\overset{(*)}{=} \left(\frac{103}{5}\right)(-1)\left(\frac{103}{7}\right)\\ &\overset{(**)}{=} \left(\frac{3}{5}\right)(-1)\left(\frac{5}{7}\right)\\ &= (-1)\cdot(-1)\cdot(-1) = -1.\end{aligned}$$

In $(*)$, we used the quadratic reciprocity (since $5 \equiv 1 \pmod 4$, we have $\left(\frac{5}{103}\right) = \left(\frac{103}{5}\right)$; since both 7 and 103 are congruent to 3 mod 4, we have $\left(\frac{7}{103}\right) = -\left(\frac{103}{7}\right)$). We used Remark 7.15 in $(**)$ (note that $103 \equiv 5 \pmod 7$).

Since $\left(\frac{35}{103}\right) = -1$, the equation $x^2 \equiv 35 \pmod{103}$ is not soluble. □

Example 7.23. Calculate

$$\left(\frac{137}{241}\right).$$

Note that both 137 and 241 are prime numbers.

Solution. We have

$$\begin{aligned}\left(\frac{137}{241}\right) &\overset{\text{quad. rec.}}{=} \left(\frac{241}{137}\right) \overset{\text{why?}}{=} \left(\frac{104}{137}\right) = \left(\frac{8\cdot 13}{137}\right) \overset{(*)}{=} \overbrace{\left(\frac{2}{137}\right)}^{\substack{1 \text{ by Thm 7.18(b)}\\ (137\equiv 1 \pmod 8)}} \left(\frac{13}{137}\right)\\ &\overset{\text{why?}}{=} \left(\frac{137}{13}\right) \overset{\text{why?}}{=} \left(\frac{7}{13}\right) \overset{\text{why?}}{=} \left(\frac{13}{7}\right) = \left(\frac{-1}{7}\right) = -1,\end{aligned}$$

where the final equality is by Theorem 7.18(b) in view of $7 \equiv 3 \pmod 4$. (In $(*)$, note that $\left(\frac{8}{137}\right) = \left(\frac{2}{137}\right)$ because $\left(\frac{4}{137}\right) = 1$.) □

Example 7.24. Let p be a prime number $\neq 5$. Show that 5 is a quadratic residue mod p if and only if p is congruent to 1 or 4 mod 5.

Solution. By the quadratic reciprocity, since $5 \equiv 1 \pmod 4$ we have

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

Thus $\left(\frac{5}{p}\right) = 1$ if and only if $\left(\frac{p}{5}\right) = 1$. The latter is equivalent to $p \equiv 1, 4 \pmod 5$, as $1, 4$ form a complete set of quadratic residues mod 5. □

Example 7.25. Determine all primes $p > 3$ such that 3 is a quadratic residue mod p. Your answer should be in terms of congruence conditions for p.

Solution. By quadratic reciprocity,

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

Thus $\left(\frac{3}{p}\right) = 1$ if and only if either

$$p \equiv 1 \pmod 4 \quad \text{and} \quad \left(\frac{p}{3}\right) = 1 \tag{7.5}$$

or

$$p \equiv -1 \pmod 4 \quad \text{and} \quad \left(\frac{p}{3}\right) = -1. \tag{7.6}$$

Note that $\left(\frac{p}{3}\right)$ is 1 (resp., -1) if and only if $p \equiv 1 \pmod 3$ (resp., $p \equiv -1 \pmod 3$). Thus

$$(7.5) \iff [\, p \equiv 1 \pmod 4 \text{ and } p \equiv 1 \pmod 3 \,] \overset{\text{Chinese rem. thm.}}{\iff} p \equiv 1 \pmod{12}.$$

Similarly,

$$(7.6) \iff [\, p \equiv -1 \pmod 4 \text{ and } p \equiv -1 \pmod 3 \,] \overset{\text{Chinese rem. thm.}}{\iff} p \equiv -1 \pmod{12}.$$

Thus 3 is a quadratic residue mod p if and only if $p \equiv \pm 1 \pmod{12}$. □

8 Week 8: Quadratic residues: Proofs of the main results I

In this week, we prove the multiplicativity of the Legendre symbol and the characterization of $\left(\frac{-1}{p}\right)$.

8.1 Multiplicativity of the Legendre symbol

At the end of this subsection we will prove Theorem 7.17. To this end, we start with a useful lemma:

Lemma 8.1. *Let p be an odd prime number and a an integer coprime to p. Suppose a is a quadratic residue mod p. Then the equation $x^2 \equiv a \pmod{p}$ has exactly two solutions mod p. More explicitly, if $x = x_0$ is a solution to $x^2 \equiv a \pmod{p}$, then the only solutions to this equation are $x \equiv \pm x_0 \mod p$, and these two solutions are distinct mod p.*

Proof. Note that the statement after "more explicitly" implies the first assertion. Suppose $x_0^2 \equiv a \pmod{p}$. If x is any integer satisfying $x^2 \equiv a \pmod{p}$, then

$$p \mid x^2 - x_0^2 = (x - x_0)(x + x_0).$$

Since p is prime, it follows that p divides $x - x_0$ or $x + x_0$, or equivalently, $x \equiv \pm x_0 \pmod{p}$.

It remains to show that x_0 and $-x_0$ are not congruent mod p. If they were congruent, then $p \mid 2x_0$, which implies that $p \mid 2$ or $p \mid x_0$. But both of these are absurd (the former because p is a prime > 2 and the latter because $x_0^2 \equiv a \not\equiv 0 \pmod{p}$). □

Recall from Examples 7.11 and 7.12 that for $p = 5, 11$ exactly half the nonzero residue classes mod p are quadratic (and the other half are not quadratic). We now show that this is true for any p:

Proposition 8.2. *Let p be an odd prime number. The numbers*

$$1^2,\ 2^2,\ \ldots,\ (\frac{p-1}{2})^2 \tag{8.1}$$

form a complete set of quadratic residues mod p. In particular, there are exactly $(p-1)/2$ quadratic residue classes.

Proof. It is clear that the numbers (8.1) is each a quadratic residue mod p. Since the numbers

$$\pm 1,\ \pm 2,\ \ldots,\ \pm\frac{p-1}{2}$$

form a complete set of residues coprime to p, the list of numbers (8.1) contains a complete set of quadratic residues mod p. It remains to show that no two of the numbers on this list are congruent mod p. Indeed, if $r^2 \equiv s^2 \pmod{p}$ with $1 \le r < s \le (p-1)/2$, then the equation $x^2 \equiv r^2 \pmod{p}$ will have $x = \pm r, \pm s$ as solutions, which contradicts Lemma 8.1. (Note that $\pm r, \pm s$ are distinct mod p.) □

We can now prove Theorem 7.17. On recalling the definition of the Legendre symbol, the result can be restated as the following:

Theorem 8.3. *Let p be an odd prime number.*

(a) *The product of two quadratic residues mod p is a quadratic residue mod p.*

(b) *The product of a quadratic residue and a quadratic non-residue mod p is a quadratic non-residue mod p.*

(c) *The product of two quadratic non-residues mod p is a quadratic residue mod p.*

Proof. First note that if $p \nmid a$ and and $p \nmid b$, then $p \nmid ab$.

(a) Let a and b be quadratic residues mod p. If $x_0^2 \equiv a$ and $y_0^2 \equiv b \mod p$, then $(x_0 y_0)^2 \equiv ab \mod p$ and hence ab is a quadratic residue mod p.

(b) Let

$$r_1, \ldots, r_{(p-1)/2}, s_1, \ldots, s_{(p-1)/2}$$

be a complete set of residues coprime to p, with each r_i a quadratic residue and each s_i a quadratic non-residue (see Proposition ; throughout, the term "quadratic residue/non-residue" means such a residue mod p). Let a be a quadratic residue. We need to show that each as_i is a quadratic non-residue. By definition of a quadratic residue, $p \nmid a$, i.e., $\gcd(a, p) = 1$. Thus

$$ar_1, \ldots, ar_{(p-1)/2}, as_1, \ldots, as_{(p-1)/2}$$

is also a complete set of residues coprime to p. By Part (a), for each i, ar_i is a quadratic residue and hence is congruent to some r_j mod p. Thus $ar_1, \ldots, ar_{(p-1)/2}$ are congruent mod p to $r_1, \ldots, r_{(p-1)/2}$, possibly in a different order. It follows that each as_i must also be congruent to s_j for some j.

(c) Let $r_1, \ldots, r_{(p-1)/2}, s_1, \ldots, s_{(p-1)/2}$ be as before. Suppose a is a quadratic non-residue. Then $ar_1, \ldots, ar_{(p-1)/2}, as_1, \ldots, as_{(p-1)/2}$ is again a complete set of residues coprime to p. By Part (b), for each i, ar_i is a quadratic non-residue and hence congruent to some s_j mod p. It follows that the ar_i must be a rearrangement of the s_j mod p. Thus each as_i must be one of the r_j. □

8.2 Euler's criterion and the determination of $\left(\frac{-1}{p}\right)$

Proposition 8.4 (Euler's criterion)**.** *Let p be an odd prime number and a an integer coprime to p. Then*

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

Proof. Let S be a complete set of residues coprime to p. For any $x_0 \in S$, there exists a unique $y_0 \in S$ such that $x_0 y_0 \equiv a \pmod{p}$. (Details: Since $\gcd(x_0, p) = 1$, the equation $x_0 y \equiv a \pmod{p}$ (in unknown y) has a unique solution mod p. Moreover, this solution is not zero mod p because $p \nmid a$. Thus the equation has a unique solution y_0 is S.) We will call y_0 the associate of x_0. It is clear from the definition that if y_0 is the associate of x_0, then x_0 is the associate of y_0. Note that x_0 is its own associate if and only if $x_0^2 \equiv a \pmod{p}$.

We will consider

$$\prod_{x \in S} x.$$

Note that by Wilson's theorem, we have

$$\prod_{x \in S} x \equiv -1 \pmod{p}.$$

We now proceed to calculate $\prod_{x\in S} x$ by breaking up S into associate pairs, as follows:

Case I: Suppose a is a quadratic non-residue mod p. Then no element of S is its own associate, so that S can be partitioned into $(p-1)/2$ associate pairs. Each associate pair multiplies out to a mod p, so that

$$\prod_{x\in S} x \equiv a^{(p-1)/2} \pmod{p}.$$

Case II: Suppose a is a quadratic residue mod p. By Lemma 8.1, the equation $x^2 \equiv a \pmod{p}$ has exactly two solutions in $\in S$, which we will call α, β; by the same lemma, $\beta \equiv -\alpha \pmod{p}$. Thus there are exactly two elements of S with the property that each is its own associate, and these two elements are α, β. The set $S\backslash\{\alpha,\beta\}$ partitions into $(p-3)/2$ associate pairs. Each pairs multiples out to $a \mod p$. We thus have

$$\prod_{x\in S} x \equiv a^{(p-3)/2}\alpha\beta \overset{(*)}{\equiv} a^{(p-3)/2}\alpha\cdot(-\alpha) \overset{(**)}{\equiv} -a^{(p-3)/2}\cdot a \equiv -a^{(p-1)/2} \pmod{p}.$$

(Note that we used $\beta \equiv -\alpha \pmod{p}$ in $(*)$ and $\alpha^2 \equiv a \pmod{p}$ in $(**)$.)

To summarize, so far we have proved:

$$-1 \overset{\text{mod } p}{\equiv} \prod_{x\in S} x \equiv \begin{cases} -a^{(p-1)/2} & \text{if } a \text{ is a quadratic residue mod } p \\ a^{(p-1)/2} & \text{if } a \text{ is a quadratic non-residue mod } p. \end{cases}$$

Thus

$$1 \overset{\text{mod } p}{\equiv} \begin{cases} a^{(p-1)/2} & \text{if } a \text{ is a quadratic residue mod } p \\ -a^{(p-1)/2} & \text{if } a \text{ is a quadratic non-residue mod } p. \end{cases}$$

This gives the desired conclusion:

$$a^{(p-1)/2} \overset{\text{mod } p}{\equiv} \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p \end{cases} = \left(\frac{a}{p}\right). \qquad \square$$

Setting $a = -1$ in Euler's criterion we obtain the determination of $\left(\frac{-1}{p}\right)$ given in Theorem 7.18(b):

Corollary 8.5. *Let p be an odd prime. Then*

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

Proof. Setting $a = -1$ is Euler's criterion we obtain

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

Since both sides of the congruence are ± 1 and $p > 2$, it follows that

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

Finally, note that $(-1)^{(p-1)/2}$ is equal to 1 (resp., -1) if and only if $(p-1)/2$ is even (resp., odd), which is equivalent to $p \equiv 1 \pmod{4}$ (resp., $p \equiv 3 \pmod{4}$). $\square$

9 Week 9: Quadratic residues: Proofs of the main results II

9.1 Gauss' lemma

Given integers $m > 0$ and a, by the least non-negative residue of a mod m we mean the smallest non-negative integer r such that $a \equiv r \pmod{m}$. Equivalently, the least non-negative residue of a mod m is the unique integer r in $\{0, 1, 2, \ldots, m-1\}$ such that $a \equiv r \pmod{m}$. That is, r is the remainder of a in division by m.

The following lemma, which is due to Gauss, will be used to prove the determination of $\left(\frac{2}{p}\right)$, and then also used in the proof of the quadratic reciprocity.

Lemma 9.1 (Gauss' lemma)**.** *Let p be an odd prime number that $a \in \mathbb{Z}$, $p \nmid a$. Let μ be the number of integers among*

$$a,\ 2a,\ \ldots,\ (\frac{p-1}{2})a \tag{9.1}$$

whose least non-negative residue mod p is greater than $p/2$. Then

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

Before the proof, let us consider an example.

Example 9.2. Take $p = 11$ and $a = 3$. We multiply $1, 2, 3, 4, 5 = (11-1)/2$ by $a = 3$ to obtain

$$3, 6, 9, 12, 15.$$

Reducing these mod 11 we obtain the least non-negative residues

$$3, 6, 9, 1, 4.$$

Out of these, two (namely, 6 and 9) are $> p/2 = 11/2$. Thus $\mu = 2$. Gauss' lemma asserts that

$$\left(\frac{3}{11}\right) = (-1)^2 = 1,$$

i.e., 3 is a quadratic residue mod 11. Note that this is indeed the case as $5^2 \equiv 3 \pmod{11}$.

Proof of Gauss' lemma (Lemma 9.1). We have

$$\prod_{i=1}^{(p-1)/2} ai \ = \ a^{(p-1)/2} \prod_{i=1}^{(p-1)/2} i. \tag{9.2}$$

On the other hand, we may calculate the left hand side mod p as follows. For every integer n, denote the difference between n and the closest multiple of p by $\|n\|$. Clearly, we have $0 \le \|n\| < p/2$ for every n. Denote the least non-negative residue of n mod p by $\{n\}$. Then

$$\{n\} = \begin{cases} \|n\| & \text{if } 0 \le \{n\} < p/2 \\ p - \|n\| & \text{if } \{n\} > p/2. \end{cases} \tag{9.3}$$

We have

$$\prod_{i=1}^{(p-1)/2} ai \overset{\text{mod } p}{\equiv} \prod_{i=1}^{(p-1)/2} \{ai\} \overset{(9.3)}{\underset{\text{mod } p}{\equiv}} (-1)^{\mu} \prod_{i=1}^{(p-1)/2} \|ai\|.$$

(Explanation for the case step: For each i such that $\{ai\} > p/2$, we used (9.3) to replace $\{ai\}$ by $-\|ai\|$. There are μ such i, by definition of μ.)

We claim that the numbers

$$\|a\|,\ \|2a\|,\ \|3a\|, \ldots,\ \|(\frac{p-1}{2})a\| \tag{9.4}$$

are simply a rearrangement of the numbers

$$1, 2, 3, \ldots, \frac{p-1}{2}. \tag{9.5}$$

Indeed, since $p \nmid a$, the $p-1$ numbers

$$\pm a, \pm 2a, \ldots, \pm(\frac{p-1}{2})a$$

form a complete set of residues coprime to p. Since $\|n\|$ is congruent to one of n or $-n$ mod p, it follows that the numbers (9.4) are distinct mod p, and in particular, they are distinct integers. Each of them appears in (9.5) (as by definition, $0 \leq \|ai\| \leq (p-1)/2$; moreover, since $p \nmid a$ and $p \nmid i$, we have $\|ai\| \neq 0$). It follows that (9.4) is indeed a rearrangement of (9.5), as claimed.

We thus have

$$\prod_{i=1}^{(p-1)/2} ai \overset{\text{mod } p}{\equiv} (-1)^{\mu} \prod_{i=1}^{(p-1)/2} \|ai\| \overset{\text{mod } p}{\equiv} (-1)^{\mu} \prod_{i=1}^{(p-1)/2} i.$$

Combining with (9.2) we get

$$a^{(p-1)/2} \prod_{i=1}^{(p-1)/2} i \ \equiv (-1)^{\mu} \prod_{i=1}^{(p-1)/2} i \pmod{p}.$$

Since $\prod_{i=1}^{(p-1)/2} i$ is a unit mod p, we get

$$a^{(p-1)/2} \equiv (-1)^{\mu} \pmod{p}.$$

In view of Euler's criterion (Proposition 8.4), this gives

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

Since each side of the last equation is ± 1 and $p > 2$, it follows that the two sides must be equal integers. □

9.2 The proof of the characterization of $\left(\frac{2}{p}\right)$

Equipped with Gauss' lemma, we will prove the characterization of when 2 is quadratic residue mod p given in Theorem 7.18(b).

We first need to introduce a useful notion. Given $\alpha \in \mathbb{R}$, its *integer part* denoted by $\lfloor \alpha \rfloor$ is defined to be the unique integer satisfying $\lfloor \alpha \rfloor \leq \alpha < \lfloor \alpha \rfloor + 1$. That is, $\lfloor \alpha \rfloor$ is the largest integer $\leq \alpha$. Thus for instance, $\lfloor 0.1 \rfloor = \lfloor 0.9 \rfloor = 0$, $\lfloor -0.1 \rfloor = -1$, and $\lfloor \alpha \rfloor = \alpha$ if and only if $\alpha \in \mathbb{Z}$. Given any positive integer m and any real number $\alpha > 0$, the number of multiples of m in the interval $[1, \alpha]$ is $\lfloor \alpha/m \rfloor$ (see Assignment 2, Extra Problems).

Proof of the characterization of $\left(\frac{2}{p}\right)$ *in Theorem 7.18(b).* We apply Gauss' lemma with $a = 2$. The numbers (9.1) are $2, 4, \ldots, p-1$, i.e., all the even positive integers $< p$. These are all already in their least non-negative residues mod p. Thus μ is the number of elements of $\{2, 4, \ldots, p-1\}$ which are $> p/2$. We have

$$\mu = |\{i \in \mathbb{Z} : \frac{p}{2} < 2i < p\}| = |\{i \in \mathbb{Z} : \frac{p}{4} < i < \frac{p}{2}\}| = \lfloor p/2 \rfloor - \lfloor p/4 \rfloor = \begin{cases} k & \text{if } \ p = 4k+1 \\ k+1 & \text{if } \ p = 4k+3. \end{cases}$$

It follows that μ is even if and only if

$$(p = 4k+1 \text{ for some even } k) \quad \text{or} \quad (p = 4k+3 \text{ for some odd } k),$$

which is equivalent to p being congruent to 1 or 7 mod 8. By Gauss' lemma,

$$\left(\frac{2}{p}\right) = (-1)^{\mu} = \begin{cases} 1 & \text{if } \ 2 \mid \mu, \text{ i.e., if } \ p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } \ 2 \nmid \mu, \text{ i.e., if } \ p \equiv 3, 5 \pmod 8. \end{cases}$$

□

10 Week 10: Proof of quadratic reciprocity, some applications, sums of squares

10.1 The proof of the quadratic reciprocity

Our goal in this subsection is to prove the quadratic reciprocity, given in Theorem 7.18(a). The proof has three ingredients, namely, Gauss' lemma (Lemma 9.1) and two other lemmas, which we give below.

Let p be an odd prime number. For brevity, we will write p' for $(p-1)/2$. For any integer $a \geq 0$, let

$$S(a, p) = \sum_{j=1}^{p'} \lfloor \frac{ja}{p} \rfloor.$$

Note that $S(a, p)$ is always an integer.

Lemma 10.1. *Let a be an integer with $p \nmid a$. Let μ be as in the statement of Gauss' lemma. That is, μ is the number of elements of*

$$a, 2a, \ldots, p'a$$

whose remainder (= least non-negative residue) mod p is $> p'$. If a is odd, then

$$S(a,p) \equiv \mu \pmod 2.$$

Proof. For each $1 \le j \le p'$, let r_j be the remainder of aj mod p. By the division algorithm, we have

$$aj = \lfloor aj/p \rfloor \cdot p + r_j.$$

Summing this over $1 \le j \le p'$, we get

$$a \sum_{j=1}^{p'} j \;=\; p \sum_{j=1}^{p'} \lfloor aj/p \rfloor \;+ \sum_{j=1}^{p'} r_j \;=\; p\,S(a,p) \;+ \sum_{j=1}^{p'} r_j\,. \tag{10.1}$$

Set

$$r'_j = \begin{cases} r_j & \text{if } r_j \le p' \\ p - r_j & \text{if } r_j > p'. \end{cases}$$

That is, r'_j is the distance of aj to the nearest multiple of p. Equation (10.1) reads

$$\begin{aligned} a \sum_{j=1}^{p'} j &= p\,S(a,p) + \sum_{j=1}^{p'} r_j \\ &= p\,S(a,p) + \sum_{\substack{j=1 \\ r_j \le p'}}^{p'} r'_j \;+ \sum_{\substack{j=1 \\ r_j > p'}}^{p'} (p - r'_j) \\ &= p\,S(a,p) + \sum_{\substack{j=1 \\ r_j \le p'}}^{p'} r'_j \;+ p\mu - \sum_{\substack{j=1 \\ r_j > p'}}^{p'} r'_j \\ &\equiv p\,S(a,p) + p\mu + \sum_{j=1}^{p'} r'_j \qquad \pmod 2, \end{aligned}$$

as $1 \equiv -1 \pmod 2$. The numbers r'_j for $1 \le j \le p'$ are merely a rearrangement of the numbers $1, \ldots, p'$ (see the proof of Lemma 9.1). Thus

$$a \sum_{j=1}^{p'} j \equiv p\,S(a,p) + p\mu + \sum_{j=1}^{p'} j \pmod 2,$$

so that

$$(a-1) \sum_{j=1}^{p'} j \equiv p\,(S(a,p) + \mu) \pmod 2.$$

Since a is odd, the left hand side is even, so that the right hand side is even. Since p is odd, it follows that $S(a,p) + \mu$ is even. Hence,

$$S(a,p) \equiv \mu \pmod 2. \qquad \square$$

Note that Lemma 10.1 together with Gauss' lemma imply that if a is odd and $p \nmid a$, then

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

We now assume p and q are two distinct odd primes. We set

$$q' := (q-1)/2 \quad \text{and} \quad p' := (p-1)/2.$$

We now have two integers $S(q,p)$ and $S(p,q)$ defined by

$$S(q,p) = \sum_{j=1}^{p'} \lfloor \frac{jq}{p} \rfloor$$

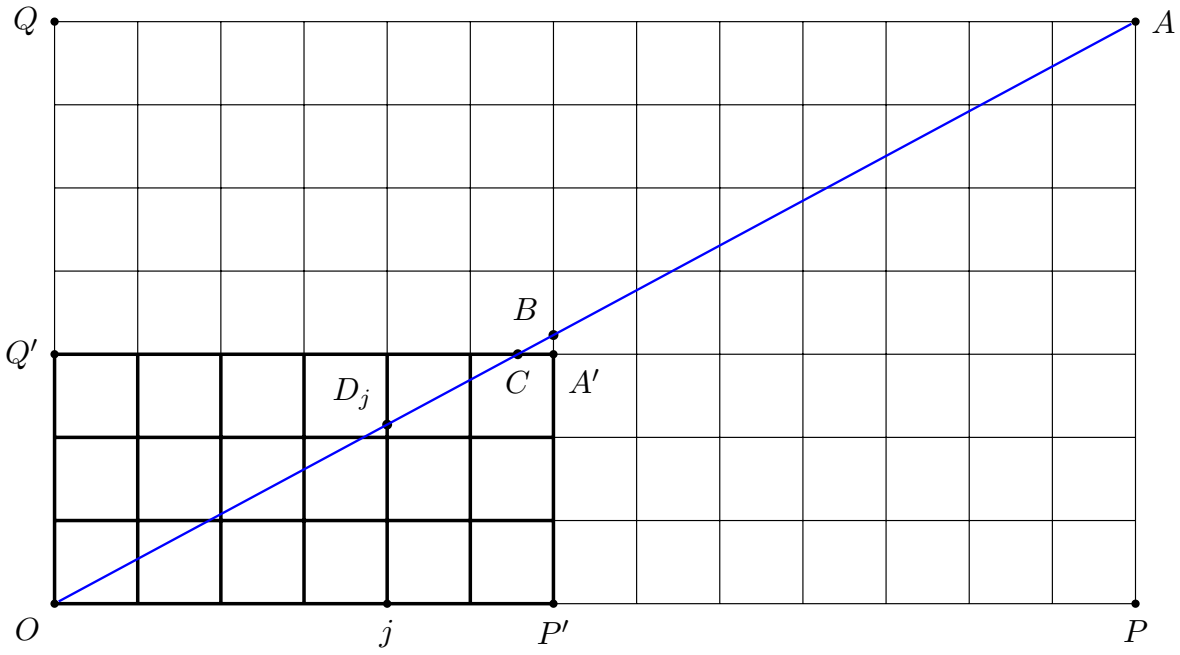
$$S(p,q) = \sum_{j=1}^{q'} \lfloor \frac{jp}{q} \rfloor.$$

The final piece of the puzzle is the following lemma.

Lemma 10.2. *With notation as above,*

$$S(q,p) + S(p,q) \; = \; p'q'.$$

Proof. We may assume $p > q$. We will establish the result using a double-counting argument, as follows. Consider the following diagram on the xy-plane:



Here,

$$O = (0,0), \quad P = (p,0), \quad Q = (0,q), \quad A = (p,q), \quad P' = (p',0), \quad Q' = (0,q'), \quad A' = (p',q').$$

The line OA is given by the equation $y = (q/p)x$. The points $B = (p', p'q/p)$ and $C = (q'p/q, q')$ are respectively the points where OA intersects the lines $x = p'$ and $y = q'$. (Our diagram is for $p = 13$ and $q = 7$.)

We will count the set I, consisting of "lattice points" (i.e., points with integer coordinates) in the rectangle $OP'A'Q'$, including those on $A'P'$ and $A'Q'$, but excluding those on the two axes. That is, I is the set of points (x, y) with $x, y \in \mathbb{Z}$, $0 < x \leq p'$, and $0 < y \leq q'$. Note that clearly I has $p'q'$ elements.

We will now count the elements of I in a different way. Since p and q are coprime integers, the line segment OA does not pass through any lattice points other that O and A (indeed, $y = (q/p)x$ is not an integer for $x = 1, 2, \ldots, p-1$ because $\gcd(p, q) = 1$). Thus we may break up I into the set of lattice points in $OP'A'Q'$ under OA, and the set of those above OA. It is easy to see that $q < p$ implies

$$q' < p'q/p < q' + 1$$

(write $q' = (q-1)/2$ and $p' = (p-1)/2$ and simplify to see this!). This shows that $B = (p', p'q/p)$ lies strictly between $A' = (p', q')$ and the lattice point $(p', q'+1)$ right above A' (see the diagram). Thus there are no lattice points in $A'BC$ expect possibly on CA'. Thus the number of elements of I under OB (i.e., the number of lattice points in $OP'A'C$) is the same as the number of all the lattice points in $OP'B$. At $x = j$, there are exactly $\lfloor jq/p \rfloor$ lattice points in $OP'B$ (indeed, we count the number of lattice points under the point $D_j = (j, jq/p)$, see the diagram; this number is the same as the number of positive integers $\leq jq/p$, which is exactly $\lfloor jq/p \rfloor$). Thus the number of elements of I under OB is $\sum_{j=1}^{p'} \lfloor jq/p \rfloor = S(q, p)$. Similarly, the number of elements of I above OB is $S(p, q)$. (The number of elements of I above OB on $y = j$ is $\lfloor jp/q \rfloor$.) Thus the total number of elements of I is $S(q, p) + S(p, q)$. We obtain the desired conclusion. □

We can now deduce the quadratic reciprocity.

Proof of the quadratic reciprocity (Theorem 7.18(a)). Let p, q be two distinct odd primes. Let $p', q', S(p, q)$, and $S(q, p)$ be as above. The statement of the quadratic reciprocity can be equivalently restated as

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

(Prove this as an exercise!) Gauss' lemma together with Lemma 10.1 gives

$$\left(\frac{p}{q}\right) = (-1)^{S(p,q)} \qquad \text{and} \qquad \left(\frac{q}{p}\right) = (-1)^{S(q,p)}.$$

Thus

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)} \overset{\text{Lemma 10.2}}{=} (-1)^{p'q'}.$$

□

10.2 Application: Infinitude of primes of the form $4k + 1$

Recall that earlier we proved that there are infinitely many primes of the form $4k + 3$. As an application of the theory of quadratic residues, we can now prove that there are infinitely many primes of the form $4k + 1$.

Proposition 10.3. *There are infinitely many prime numbers that are congruent to 1 mod 4.*

Proof. Let $p_1, p_2, \ldots, p_n$ be n prime numbers. We shall show that there exists a prime number $q \equiv 1 \pmod 4$ which is not any of the p_i. Let

$$N = (2p_1p_2 \cdots p_n)^2 + 1.$$

Let q be a prime divisor of N (note that $N > 1$ so it has a prime divisor). The reader can easily check that q is not any of the p_i (make sure you do this!). We will show that q is congruent to 1 mod 4. Since N is odd, q is odd. Since $q \mid (2p_1p_2 \cdots p_n)^2 + 1$, we have

$$(2p_1p_2 \cdots p_n)^2 \equiv -1 \pmod q,$$

so that -1 is a quadratic residue mod q. Thus $q \equiv 1 \pmod 4$. □

10.3 Application to Diophantine equations

We may use the theory of quadratic residues to show that some Diophantine equations do not have any solutions. We will illustrate this by two examples.

Example 10.4. Show that

$$x^2 - 23y^2 = -1$$

has no solutions in $\mathbb{Z}$.

Solution. Suppose there exist integers x, y satisfying the equation. Reducing the equation modulo the prime 23, we get

$$x^2 \equiv -1 \pmod{23},$$

so that -1 is a quadratic residue mod 23. But 23 is a prime number congruent to 3 mod 4, and hence -1 is not a quadratic residue mod 23. We have a contradiction. □

Example 10.5. Show that the curve defined by

$$86y^3 - 3x^2 = 2$$

does not pass through any points with integer coordinates.

Solution. We need to show that the equation

$$86y^3 - 3x^2 = 2$$

has no solutions in $\mathbb{Z}$. Suppose the equation has solutions $x, y \in \mathbb{Z}$. Reducing the equation mod 43, we get

$$-3x^2 \equiv 2 \pmod{43}.$$

Multiplying by $14 = (-3)^{-1} \mod 43$ (note that $(-3)(14) = -42 \equiv 1 \mod 43$), we get

$$x^2 \equiv 2 \cdot 14 \equiv 28 \pmod{43}.$$

But there is no x satisfying the last equation as

$$\left(\frac{28}{43}\right) = \left(\frac{7}{43}\right)\left(\frac{4}{43}\right) = \left(\frac{7}{43}\right) = -\left(\frac{43}{7}\right) = -\left(\frac{1}{7}\right) = -1.$$ □

10.4 Sums of squares

We now consider the following classical problem.

Problem 10.6. Given a positive integer m, determine if m is a sum of two squares. That is, determine if

$$m = a^2 + b^2$$

for some $a, b \in \mathbb{Z}$.

An answer to this is given by the following theorem.

Theorem 10.7. *A positive integer m is a sum of two squares if and only if for every prime number $p \equiv 3 \pmod 4$, the exponent of p in the prime factorization of m is even.*

For example, any number with no prime divisor congruent to 3 mod 4 is a sum of two squares. The number $m = 2 \times 7^3 \times 13^3$ is not a sum of two squares, since the exponent of 7 (which is a prime of the form $4k+3$) in m is odd. On the other hand, $m = 2 \cdot 7^4 13^3$ is a sum of two squares.

In this subsection, we will prove the "only if" implication of Theorem 10.7. That is, we will prove that if m is a sum of two squares, then every prime of the form $4k+3$ appears with an even exponent in the prime factorization of m. We shall see that this is a consequence of the characterization of when -1 is a quadratic residue mod a prime number. The key is the following lemma.

Lemma 10.8. *Let $a, b \in \mathbb{Z}$. Suppose $a^2 + b^2$ is divisible by a prime number $p \equiv 3 \pmod 4$. Then $p \mid a$ and $p \mid b$.*

Proof. Let $m = a^2 + b^2$. We first observe that either p divides both a, b, or p doesn't divide any of a, b. Indeed, say $p \mid a$, then $p \mid m - a^2$ because $p \mid a, m$. That is, p divides b^2. Since p is prime, it follows that p divides b.

Suppose $p \nmid a$ and $p \nmid b$. We have

$$a^2 \equiv -b^2 \pmod p.$$

Thus

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

But -1 is not a quadratic residue mod p since $p \equiv 3 \pmod 4$. □

Exercise 10.1. Determine if the following statement true or false: If a, b are coprime integers, then every odd prime divisor of $a^2 + b^2$ is congruent to 1 mod 4.

We can now establish the "only if" implication in Theorem 10.7.

Proposition 10.9. *If $m > 0$ is a sum of two squares, then every prime of the form $4k+3$ appears with an even exponent in the prime factorization of m.*

Proof. Suppose the statement is false. Let m be the smallest counter-example to the statement. Thus m is the *smallest* positive integer that satisfies the following two conditions:

(i) m is a sum of two squares;

(ii) there exists a prime number $p \equiv 3 \pmod 4$ such that the exponent of p in the prime factorization of m is odd.

Note that in particular, (ii) implies that $p \mid m$. By Lemma 10.8, we have $p \mid a$ and $p \mid b$. Write $a = pa'$ and $b = pb'$ (note that a', b' are integers). Then

$$m = a^2 + b^2 = p^2(a'^2 + b'^2),$$

so that $p^2 \mid m$. Write $m = p^2 m'$, where m' is an integer. Since the exponent of p in the prime factorization of m is odd, the exponent of p in the prime factorization of $m' = m/p^2$ is also odd. We have

$$p^2 m' = p^2(a'^2 + b'^2),$$

so that

$$m' = a'^2 + b'^2.$$

Thus m' is a also sum of two squares. It follows that m' is also a counter-example to the statement of the proposition. This is a contradiction as $0 < m' < m$ and by definition, m is the smallest possible counter-example to the statement. □

Remark 10.10. The method of the proof of Proposition 10.9 is called the method of *infinite descent*. Suppose we are trying to prove some statement P about positive integers. The general structure of the argument is as follows: Suppose P is false. Let $m \in \mathbb{Z}_{>0}$ be the smallest counter-example to P. If we succeed in arguing that there exists an even smaller counter-example $0 < m' < m$, then we have a contradiction.

11 Week 11: Sums of squares (continued), Pythagorean triples

11.1 Sums of squares (continued)

In this subsection we will prove the remaining implication of Theorem 10.7, which asserts the following:

Theorem 11.1. *Let m be a positive integer with the property that for every prime $p \equiv 3 \pmod 4$, the exponent of p in the prime factorization of m is even. Then m is a sum of two squares.*

The proof of this has two ingredients. The first ingredient is the following interesting simple observation.

Lemma 11.2. *Suppose that m and n are sums of two squares. Then mn is also a sum of two squares.*

Proof. A direct computation shows

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \tag{11.1}$$

(Just expand the two sides!) □

By induction on k, if each of $m_1, m_2, \ldots, m_k$ is a sum of two squares, the so is their product $m_1 m_2 \cdots m_k$.

The second ingredient of Theorem 11.1, which is the core case of the theorem, is the following result. This result is usually referred to Fermat's theorem on sums of squares, although the first proof of it was given by Euler.

Theorem 11.3. *Let p be a prime number congruent to 1 mod 4. Then p is a sum of two squares.*

The next subsection is dedicated to the proof of this result. Let us take it for granted here and deduce Theorem 11.1.

Proof of Theorem 11.1 assuming Theorem 11.3. Let m be as in the statement. Then m can be expressed as

$$m = n^2 p_1 \cdots p_k,$$

where $n \in \mathbb{Z}$ and each p_i is either 2 or a prime number congruent to 1 mod 4. Note that $2 = 1^2 + 1^2$. In view of Theorem 11.3, it follows that every p_i is a sum of two squares. By Lemma 11.2, their product $p_1 \cdots p_k$ is a sum of two squares. Hence $n^2 p_1 \cdots p_k = m$ is also a sum of two squares. □

Example 11.4. Express $m = 2 \cdot 37 \cdot 13 \cdot 3^4$ as a sum of two squares.

Solution. We have $2 = 1^2 + 1^2$, $37 = 6^2 + 1^2$, and $13 = 3^2 + 2^2$. By successive applications of (11.1), we have

$$2 \cdot 37 = (1 \cdot 6 - 1 \cdot 1)^2 + (1 \cdot 1 + 1 \cdot 6)^2 = 5^2 + 7^2$$

and

$$2 \cdot 37 \cdot 13 = (5^2 + 7^2)(3^2 + 2^2) = (15 - 14)^2 + (10 + 21)^2 = 1^2 + 31^2.$$

Thus

$$m = (1^2 + 31^2)9^2 = 9^2 + 279^2.$$ □

Remark 11.5. (For interested students with familiarity with complex number; not needed for the assessments.) The formula (11.1) may seem surprising and unmotivated at first. The formula can be contextualized in terms of the notion of the norm or absolute value of complex numbers. Given a complex number $z = a + bi$ with $a, b \in \mathbb{R}$, recall that one defines $|z| = \sqrt{a^2 + b^2}$. Setting $z = a + bi$ and $w = c + di$, we have

$$zw = (ac - bd) + (ad + bc)i,$$

so that

$$|zw|^2 = (ac - bd)^2 + (ad + bc)^2.$$

On the other hand,

$$|z|^2 |w|^2 = (a^2 + b^2)(c^2 + d^2).$$

Comparing these with (11.1), we see that (11.1) can be rewritten as

$$|z|^2 |w|^2 = |zw|^2,$$

which is equivalent to the property

$$|z| \cdot |w| = |zw|$$

of norms of complex numbers.

11.2 Sums of squares (continued): Proof of Fermat's theorem

Our goal in this subsection is to prove that every prime number congruent to 1 mod 4 is a sum of two squares. This will complete the proof of Theorem 11.1 and hence Theorem 10.7. The proof we shall give is due to Euler and uses Fermat's method of descent.

We shall fix a prime number p congruent to 1 mod 4. The final goal is to show that p is a sum of two squares. We shall approach this in two steps:

- Step 1: Show that some multiple of p is a sum of two squares; more precisely, show that

$$a^2 + b^2 = pk$$

for some integers a, b, k with $0 < k < p$. The final goal is to show that k can be taken to be 1.

- Step 2: Given any integers $a, b, k \in \mathbb{Z}$ with $1 < k < p$ and

$$a^2 + b^2 = pk,$$

show that there exist integers a_1, b_1, k_1 with $0 < k_1 < k$ and

$$a_1^2 + b_1^2 = pk_1.$$

Step two is called *the descent procedure*. If $k_1 > 1$, then we can feed $a_1^2 + b_1^2 = pk_1$ into the descent procedure and get a_2, b_2, k_2 with $0 < k_2 < k_1$ and $a_2^2 + b_2^2 = pk_2$. If $k_2 > 1$, we apply the descent procedure again. Continuing in this fashion, after a finite number r of steps we arrive at $k_r = 1$ and integers a_r, b_r such that

$$a_r^2 + b_r^2 = pk_r = p.$$

We now proceed to carry out the two steps of the argument.

11.2.1 Step 1

This is not difficult: Indeed, since $p \equiv 1 \pmod 4$, we know that -1 is a quadratic residue mod p. Since $1, \ldots, p-1$ form a complete set of residues prime to p, there exists $1 \leq a \leq p-1$ such that $a^2 \equiv -1 \pmod p$, i.e., such that

$$a^2 + 1 = pk$$

for some integer k. Moreover,

$$0 < a^2 + 1 \leq (p-1)^2 + 1 < p^2,$$

so that $0 < k < p$.

11.2.2 Step 2: The descent procedure

The is the really interesting part of the proof. The input of the procedure is a triple of integers (a, b, k) with $1 < k < p$ and

$$a^2 + b^2 = pk. \tag{11.2}$$

The outputs will be a triple of integers (a_1, b_1, k_1) with $0 < k_1 < k$ and $a_1^2 + b_1^2 = pk_1$.

First, let r, s be integers such that

$$a \equiv r \pmod{k}, \qquad b \equiv s \pmod{k}, \quad \text{and} \qquad |r|, |s| \leq k/2. \tag{11.3}$$

Note that such r, s exist since $\{l \in \mathbb{Z} : -k/2 \leq l \leq k/2\}$ contains a complete set of residues mod k. The integers $ar + bs$, $as - br$, and $r^2 + s^2$ are all divisible by k as

$$\begin{aligned} ar + bs &\equiv a^2 + b^2 \equiv 0 \pmod{k} \\ as - br &\equiv ab - ba \equiv 0 \pmod{k} \\ r^2 + s^2 &\equiv a^2 + b^2 \equiv 0 \pmod{k} \end{aligned} \tag{11.4}$$

by (11.3) and (11.2). We have

$$(ar + bs)^2 + (as - br)^2 = a^2r^2 + b^2s^2 + a^2s^2 + b^2r^2 = (a^2 + b^2)(s^2 + r^2) = pk(s^2 + r^2).$$

Hence,

$$(\frac{ar + bs}{k})^2 + (\frac{as - br}{k})^2 = p \cdot \frac{s^2 + r^2}{k},$$

where all three fractions are actually integers. Set

$$a_1 = \frac{ar + bs}{k}, \qquad b_1 = \frac{as - br}{k}, \qquad k_1 = \frac{s^2 + r^2}{k}.$$

We claim that

$$0 < k_1 < k,$$

so that (a_1, b_1, k_1) satisfies the desired properties for the outcome of the descent procedure. Indeed, by (11.3) we have

$$k_1 = \frac{s^2 + r^2}{k} \leq \frac{k^2/4 + k^2/4}{k} = k/2 < k.$$

It remains to show that $k_1 > 0$. For this, we need to show that either r or s is nonzero. Suppose $r = s = 0$. Then $k \mid a$ and $k \mid b$, so that

$$k^2 \mid a^2 + b^2 = kp$$

and thus $k \mid p$. But this is absurd since p is prime and $1 < k < p$. (Note that this is the only place in the argument that we used the assumption that $k > 1$.) □

Summary of the descent procedure: Given $a, b, k \in \mathbb{Z}$ such that $a^2 + b^2 = kp$ and $1 < k < p$, find r, s satisfying

$$a \equiv r \pmod{k}, \qquad b \equiv s \pmod{k}, \quad \text{with} \qquad |r|, |s| \leq k/2.$$

Set

$$a_1 = \frac{ar+bs}{k}, \qquad b_1 = \frac{as-br}{k}, \qquad k_1 = \frac{s^2+r^2}{k}.$$

Then a_1, b_1, k_1 are integers, $0 < k_1 < k$ and $a_1^2 + b_1^2 = pk_1$. If $k_1 > 1$, we iterate the descent procedure by feeding a_1, b_1, k_1 into the procedure as the new a, b, k. We stop when $k_1 = 1$.

Example 11.6. Starting from

$$557^2 + 55^2 = 26 \cdot 12049,$$

apply the descent procedure (as many times as needed) to write the prime 12049 as a sum of two squares.

Solution. We use the notation introduced above. Set $a = 557$, $b = 55$, and $k = 26$. We have

$$557 \equiv 11 \pmod{26}, \quad 55 \equiv 3 \pmod{26}$$

so we set $r = 11$ and $s = 3$ (note that these are indeed in the interval $[-k/2, k/2]$). Then

$$\begin{aligned} k_1 &= \frac{r^2+s^2}{k} = \frac{121+9}{26} = 5 \\ a_1 &= \frac{ar+bs}{k} = \frac{557 \cdot 11 + 55 \cdot 3}{26} = 242 \\ b_1 &= \frac{as-br}{k} = \frac{557 \cdot 3 - 55 \cdot 11}{26} = 41 \end{aligned}$$

satisfy $242^2 + 41^2 = 5 \cdot 12049$. We apply the descent procedure again, this time setting $a = 242$, $b = 41$, and $k = 5$. We have

$$a = 242 \overset{(\mathrm{mod}\ 5)}{\equiv} 2 = r, \qquad b = 41 \overset{(\mathrm{mod}\ 5)}{\equiv} 1 = s.$$

Then we have

$$\begin{aligned} k_1 &= \frac{r^2+s^2}{k} = \frac{2^2+1^2}{5} = 1 \\ a_1 &= \frac{ar+bs}{k} = \frac{242 \cdot 2 + 41 \cdot 1}{5} = 105 \\ b_1 &= \frac{as-br}{k} = \frac{242 \cdot 1 - 41 \cdot 2}{5} = 32. \end{aligned}$$

We have

$$105^2 + 32^2 = 12049. \qquad \square$$

Example 11.7. Apply the descent procedure to $97^2 + 1^2 = 941 \cdot 10$ to write the prime 941 as a sum of two squares.

Solution. We adopt the same notation as before. Set $a = 97$, $b = 1$, $k = 10$. Reducing mod $k = 10$, we have $r = -3$ and $s = 1$ (we took $r = -3$ because we want $|r| \leq k/2$). Then the output of the descent procedure is

$$k_1 = \frac{r^2+s^2}{k} = 1, \quad a_1 = \frac{ar+bs}{k} = 29, \quad b_1 = \frac{as-br}{k} = 10.$$

Since $k_1 = 1$, we do not need any more iterations of the descent procedure. We have

$$29^2 + 10^2 = 1 \cdot 941 = 941. \qquad \square$$

11.3 Pythagorean triples I: The elementary approach

Our goal in this subsection is to study the Diophantine equation

$$a^2 + b^2 = c^2$$

in the integers. That is, we are looking for all triples of integers (a, b, c) that satisfy the equation. Such triples are called *Pythagorean triples* because of the obvious relation to the Pythagorean theorem in geometry: The triples with $a, b, c \in \mathbb{Z}_{>0}$ correspond to right triangles with integral side lengths.

We start by three easy observations. The first is that if (a, b, c) is a Pythagorean triple, then so are $(\pm a, \pm b, \pm c)$. We may thus focus our attention on the triples with $a, b, c \geq 0$. The second observation is that among these, those with $abc = 0$ are the triples of the form $(a, 0, a)$ and $(0, b, b)$. We may thus assume from this point on that $a, b, c > 0$. The third observation is that for every a, b, c and $d \neq 0$,

$$a^2 + b^2 = c^2 \qquad \Longleftrightarrow \qquad (ad)^2 + (bd)^2 = (cd)^2.$$

Let us call a Pythagorean triple (a, b, c) *primitive* if $\gcd(a, b, c) = 1$. By the above observation, if (a', b', c') is a Pythagorean triple and $d = \gcd(a', b', c')$, then $(a'/d, b'/d, c'/d)$ is a primitive Pythagorean triple. On the other hand, if (a, b, c) is a Pythagorean triple, then so is (ad, bd, cd) for every integer d. Thus we may focus on finding all primitive Pythagorean triples, as we can find all Pythagorean triples by scaling the primitive ones.

Thus from this point on, we focus on trying to find all the primitive Pythagorean triples in the positive integers, i.e., triples $(a, b, c) \in \mathbb{Z}^3$ such that

$$a^2 + b^2 = c^2 \qquad (a, b, c \in \mathbb{Z}_{>0},\ \gcd(a, b, c) = 1). \tag{11.5}$$

We claim one of a, b is even and the other is odd. Indeed, for this we need to rule out the possibility that a, b are both even or both odd. They cannot both be even, as then c will also be even, which violates $\gcd(a, b, c) = 1$. Also, a and b cannot both be odd, for then $a^2, b^2 \equiv 1 \pmod 4$, and so

$$c^2 = a^2 + b^2 \equiv 1 + 1 \equiv 2 \pmod 4,$$

which is absurd since there is no integer c such that $c^2 \equiv 2 \pmod 4$.

We will assume without loss of generality that a is odd and b is even (note that the equation is symmetric in a, b). We have

$$a^2 = c^2 - b^2 = (c - b)(c + b). \tag{11.6}$$

We claim that $c - b$ and $c + b$ are coprime. Indeed, if p is a common prime divisor of $c - b$ and $c + b$, then p divides $(c + b) + (c - b) = 2c$ and $(c + b) - (c - b) = 2b$. Note that $p \neq 2$ since $c - b$ and $c + b$ are odd (as c is odd and b is even). It follows that $p \mid b$ and $p \mid c$, which then implies that $p \mid a$, which is absurd since $\gcd(a, b, c) = 1$. Thus $c - b$ and $c + b$ cannot have any common prime divisor, hence $c - b$ and $c + b$ are coprime. Combining with the fact that $(c - b)(c + b)$ is a square (by (11.6)), it follows that each of $c - b$ and $c + b$ must be a square (think about the prime factorizations to see this!). That is, we have

$$c - b = r^2 \quad \text{and} \quad c + b = s^2$$

for some integers $r, s \geq 0$. Then

$$b = (s^2 - r^2)/2, \quad c = (s^2 + r^2)/2,$$

and

$$a^2 = (c - b)(c + b) = r^2 s^2.$$

On recalling that $a, b, c > 0$, it follows that

$$a = rs$$

and $s > r \geq 1$. Since a is odd, r and s are odd. Moreover, r, s must be coprime. Indeed, if $p \mid r$ and $p \mid s$ for some prime p (which will have to be odd because r, s are odd), then $p \mid s^2 \pm r^2 = 2c, 2b$. This would imply that $p \mid b$ and $p \mid c$, and hence $p \mid a$. This is a contradiction since $\gcd(a, b, c) = 1$.

We have proved that every Pythagorean triple (a, b, c) with

$$a, b, c > 0, \quad \gcd(a, b, c) = 1, \quad 2 \nmid a \qquad (\text{hence } 2 \mid b) \tag{11.7}$$

is of the form

$$a = rs, \quad b = \frac{s^2 - r^2}{2}, \quad c = \frac{s^2 + r^2}{2} \tag{11.8}$$

for some integers

$$s > r \geq 1, \quad \gcd(r, s) = 1, \quad 2 \nmid rs.$$

Conversely, given any such r, s, defining a, b, c by (11.8) we obtain a Pythagorean triple (a, b, c) with (11.9). (Indeed, a direct computation shows a, b, c satisfy $a^2 + b^2 = c^2$. Moreover, since r, s are both odd, a, b, c are integers and a is odd. Finally, the condition $\gcd(r, s) = 1$ implies that $\gcd(a, b, c) = 1$.)

For convenience, we record the result.

Proposition 11.8. *The general solution to the equation*

$$a^2 + b^2 = c^2$$

with $a, b, c \in \mathbb{Z}_{>0}$, $\gcd(a, b, c) = 1$ *and* $2 \nmid a$ *is given by*

$$a = rs, \quad b = \frac{s^2 - r^2}{2}, \quad c = \frac{s^2 + r^2}{2},$$

where r, s *are coprime odd integers with* $s > r \geq 1$.

Example 11.9. The table below lists the first few primitive Pythagorean triples (a, b, c).

r	s	$a = rs$	$b = (s^2 - r^2)/2$	$c = (s^2 + r^2)/2$
1	3	3	4	5
1	5	5	12	13
1	7	7	24	25
3	5	15	8	17
3	7	21	20	29

Example 11.10. Notice that in the first three triples in the above table we have $c = b + 1$. Let us try to find all primitive Pythagorean triples $(a, b, c) \in \mathbb{Z}^3_{>0}$ with $c = b + 1$ (note that in fact, the condition $c = b + 1$ forces the triple to be primitive). Since c and b have different parity, a, c must be odd and b even (as otherwise, a is even and b, c are odd). Thus a, b, c must be as in Proposition 11.8 for some odd coprime integers $s > r \geq 1$. Then

$$c - b = (s^2 + r^2)/2 - (s^2 - r^2)/2 = r^2.$$

Thus $c - b = 1$ if and only if $r = 1$. It follows that there are infinitely many Pythagorean triples $(a, b, c) \in \mathbb{Z}_{>0}$ such that $c = b + 1$. A complete list of them is given by

$$a = s, \quad b = (s^2 - 1)/2, \quad c = (s^2 + 1)/2$$

where s can be any odd integer > 1.

11.4 Pythagorean triples II: The connection to rational points on the unit circle

Suppose $a, b, c \in \mathbb{Z}$ satisfy

$$a^2 + b^2 = c^2.$$

Assume $c \neq 0$. Dividing the above equation by c^2, we get

$$(a/c)^2 + (b/c)^2 = 1.$$

Thus the pair $(x, y) = (a/c, b/c)$ is a rational solution to the equation

$$x^2 + y^2 = 1.$$

This equation is the equation of the unit circle in $\mathbb{R}^2$, i.e., the circle of radius 1 centred at the origin. The point $(x, y) = (a/c, b/c)$ is a rational point (i.e., a point with rational coordinates) on this circle. We thus have a map (or function)

$$\begin{array}{ccc} \left\{ \begin{array}{l} \text{Pythagorean triples} \\ (a,b,c) \in \mathbb{Z}^3 \text{ with } c \neq 0 \end{array} \right\} & \to & \left\{ \begin{array}{l} \text{Rational points on the} \\ \text{unit circle } x^2 + y^2 = 1 \end{array} \right\} \\ (a, b, c) & \mapsto & (a/c, b/c). \end{array} \tag{11.9}$$

For example, this map sends the Pythagorean triple $(3, 4, 5)$ to the point $(3/5, 4/5)$ on the unit circle. Note that the map sends the triple $(6, 8, 10)$ (obtained by scaling $(3, 4, 5)$) also to the same point $(3/5, 4/5)$ on the unit circle. More generally, if $(a', b', c') = (ad, bd, cd)$, then the triples (a', b', c') and (a, b, c) are mapped to the same point on the unit circle. In fact, it is not hard to show that two Pythagorean triples are mapped to the same point on the unit circle *if and only if* the two triples are obtained from each other by scaling.

Given a rational point $P = (x, y)$ on the unit circle, we may write $x = a/c$ and $y = b/c$ for some integers a, b, c where $c \neq 0$ is a common denominator for x and y. Since $(a/c, b/c)$ is on the unit circle, we have

$$(a/c)^2 + (b/c)^2 = 1,$$

which implies

$$a^2 + b^2 = c^2$$

and so we obtain a Pythagorean triple (a, b, c) with $c \neq 0$. The map (11.9) sends the triple (a, b, c) to the point P. This shows that the map (11.9) is surjective.

Thus (11.9) gives a bijection

$$\left\{\begin{array}{l}\text{Pythagorean triples}\\ (a,b,c)\in\mathbb{Z}^3 \text{ with } c\neq 0,\\ \text{up to scaling}\end{array}\right\} \xrightarrow{\text{bijection}} \left\{\begin{array}{l}\text{Rational points on the}\\ \text{unit circle } x^2+y^2=1\end{array}\right\} \tag{11.10}$$
$$(a,b,c) \longmapsto (a/c, b/c).$$

The term "Pythagorean triples up to scaling" can be made precise using the notion of equivalence classes, but let us not worry about that.[4] Intuitively, this means that we think of all the Pythagorean triples that can be obtained from each other by scaling as the same triple.

Thus, in order to find all Pythagorean triples, we can instead try to find all rational points on the unit circle. If we manage to do the latter, from each rational point (x, y) on the unit circle (i.e., a rational solution to $x^2 + y^2 = 1$), by "clearing the denominators" (i.e., by multiplying the equation by a common denominator of x^2 and y^2), we obtain an integral solution to $a^2+b^2 = c^2$. This way, up to scaling, we obtain all Pythagorean triples with $c \neq 0$.

In the next class we will find all the rational point on the unit circle.

12 Week 12: Rational points on conics

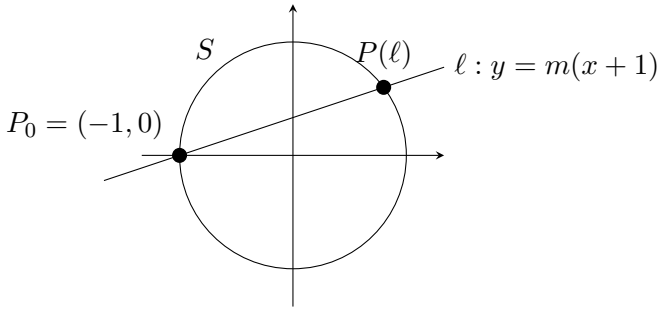
12.1 Rational points on the unit circle

Our goal in this subsection is to find all rational solutions to

$$x^2 + y^2 = 1.$$

This equation defines the circle of radius 1 in $\mathbb{R}^2$ centred at the origin (i.e., the unit circle), which we will denote by S. In other words, our goal is to find all rational points (= points with rational coordinates) on the unit circle. We will use the notation $S(\mathbb{Q})$ to denote the set of rational points of S.

We note that S certainly has some rational points, for example, $(0, \pm 1)$, $(\pm 1, 0)$, and $(\pm 3/5, \pm 4/5)$. We fix one such point and call it $P_0 = (x_0, y_0)$. In what follows, we have taken $P_0 = (-1, 0)$.



[4] Here is the precise version: Define a relation on the set of Pythagorean triples (a, b, c) with nonzero c as follows. Given two such Pythagorean triples (a, b, c) and (a', b', c'), set $(a, b, c) \sim (a', b', c')$ if and only if $(a', b', c') = (ad, bd, cd)$ for some nonzero $d \in \mathbb{Q}$. This is an equivalence relation. The precise meaning of the domain of (11.10) is the set of equivalence classes of this relation.

Let ℓ be a line that passes through P_0. It is clear that the line ℓ meets S at two points, one of which, of course, is P_0 (see the diagram). We can find the second intersection point, which we denote by $P = P(\ell)$, as follows (the calculation will also confirm our geometric observation that there are two intersection points!). For non-vertical ℓ, let m be the slope of ℓ. Then ℓ is given by the equation

$$\ell : \quad y = m(x+1).$$

To find the points of intersection of ℓ with S, we substitute $y = m(x-1)$ in $x^2 + y^2 = 1$ to get

$$x^2 + (m(x+1))^2 = 1,$$

which after expanding becomes

$$(m^2+1)x^2 + 2mx + m^2 - 1 = 0. \tag{12.1}$$

This is a quadratic equation in x, the solutions to which are the x-coordinates of $\ell \cap S$. Since the line ℓ passes through $P_0 = (-1, 0)$, we know that $x_0 = -1$ is a solution to (12.1). Since the product of the two roots is $(m^2-1)/(m^2+1)$ (see Remark 12.1 below), it follows that the other root, denoted by x_1 (= the x-coordinate of the second point of intersection $P = (x_1, y_1)$), is given by

$$x_1 = \frac{1-m^2}{m^2+1}.$$

Substituting in the equation of ℓ we obtain

$$y_1 = m(x_1+1) = m(\frac{1-m^2}{m^2+1} + 1) = \frac{2m}{m^2+1}.$$

We have a map

$$\left\{\begin{matrix}\text{lines passing} \\ \text{through } P_0\end{matrix}\right\} \longrightarrow S \qquad \ell \mapsto P(\ell) = (\frac{1-m^2}{m^2+1}, \frac{2m}{m^2+1}) \quad (m = \text{slope of } \ell). \tag{12.2}$$

(Strictly speaking, our computations were only valid for non-vertical lines (i.e., lines with a finite slope), and they give the map from the set of non-vertical lines at P_0 to $S \setminus \{P_0\}$. We separately send the vertical line to P_0. Our formula is consistent with this, provided that the value of $(\frac{1-m^2}{m^2+1}, \frac{2m}{m^2+1})$ at $m = \infty$ is defined to be its limit as $m \to \infty$.)

We make three important observations about this map:

(i) It is a bijection. Indeed, the inverse to (12.2) is obtained by sending a point $P \in S$ to the line PP_0.[5]

(ii) If $P(\ell)$ is a rational point, then ℓ is either vertical (infinite slope) or a rational slope. Indeed, if $P(\ell) \neq P_0$, writing $P(\ell)$ as (x_1, y_1) the slope of ℓ is

$$m = (y_1 - y_0)/(x_1 - x_0) = y_1/(x_1+1),$$

which is rational since x_0, y_0, x_1, y_1 are all rational. On the other hand, if $P(\ell) = P_0$, then ℓ is vertical.

[5] Again, strictly speaking, this only gives the inverse for $P \neq P_0$. We send $P = P_0$ separately to the tangent line at P_0.

(iii) If ℓ is vertical or has a rational slope, then $P(\ell)$ is a rational point. This is seen by our formula

$$P(\ell) = (\frac{1-m^2}{m^2+1}, \frac{2m}{m^2+1}) \qquad (m = \text{slope of } \ell).$$

Putting these observations together, we obtain that (12.2) gives a bijection

$$\left\{\begin{matrix}\text{lines passing through} \\ P_0 \text{ with rational or} \\ \text{infinite slope}\end{matrix}\right\} \longrightarrow S(\mathbb{Q}) \qquad \ell \mapsto P(\ell) = (\frac{1-m^2}{m^2+1}, \frac{2m}{m^2+1}) \quad (m = \text{slope of } \ell). \tag{12.3}$$

Thus

$$\begin{aligned} S(\mathbb{Q}) &= \{(\frac{1-m^2}{m^2+1}\,, \frac{2m}{m^2+1}) : m \in \mathbb{Q} \text{ or } m = \infty\} \\ &= \{(\frac{1-m^2}{m^2+1}\,, \frac{2m}{m^2+1}) : m \in \mathbb{Q}\} \cup \{P_0\}. \end{aligned}$$

We have completed the task of finding all rational points on the unit circle. For example, setting $m = 1/3$ we obtain the point

$$(\frac{1-(1/3)^2}{(1/3)^2+1}\,, \frac{2/3}{(1/3)^2+1}) = (\frac{4}{5}, \frac{3}{5}).$$

Multiplying

$$(\frac{4}{5})^2 + (\frac{3}{5})^2 = 1$$

by 5^2, we obtain

$$4^2 + 3^2 = 5^2,$$

i.e., the Pythagorean triple $(4, 3, 5)$.

More generally, writing $m = u/v$ with $u, v \in \mathbb{Z}$, $v > 0$, and $\gcd(u, v) = 1$ (note that every m can be written uniquely in thos form), we have

$$(\frac{1-m^2}{m^2+1}\,, \frac{2m}{m^2+1}) = (\frac{v^2-u^2}{u^2+v^2}\,, \frac{2uv}{u^2+v^2})$$

This is a point on the unit circle, so that

$$(\frac{v^2-u^2}{u^2+v^2})^2 + (\frac{2uv}{u^2+v^2})^2 = 1.$$

Multiplying by $(u^2+v^2)^2$, we get

$$(v^2-u^2)^2 + (2uv)^2 = (u^2+v^2)^2,$$

i.e., the Pythagorean triple

$$a = v^2 - u^2,\ b = 2uv,\ c = v^2 + u^2.$$

By §11.4, letting u and v vary, we obtain all Pythagorean triples with $c \neq 0$ up to scaling.

Remark 12.1. Let $x = \alpha$ and $x = \beta$ be the solutions of a quadratic equation

$$ax^2 + bx + c = 0.$$

We claim that

$$\alpha\beta = c/a \quad \text{and} \quad \alpha + \beta = -b/a.$$

Indeed, we have

$$ax^2 + bx + c = A(x - \alpha)(x - \beta),$$

a priori, for a polynomial A. Both $ax^2 + bx + c$ and $(x - \alpha)(x - \beta)$ have degree 2, so that A must be a constant. Comparing the coefficients of x^2 on the two sides, we get $A = a$. Thus

$$ax^2 + bx + c = a(x - \alpha)(x - \beta).$$

The constant term on the right is $a\alpha\beta$. This must match the constant term on the left, so that $c = a\alpha\beta$, as desired. Similarly, comparing the coefficients of x on the two sides, we get $b = -a(\alpha + \beta)$.

12.2 Rational points on conics

A conic section (or for short, a conic) is a curve that is either a hyperbola, ellipse (in particular, a circle), or a parabola.[6] Saying it more explicitly, a conic is a curve C defined by an equation of the form

$$f(x, y) = 0$$

in the xy-plane, where $f(x, y)$ is a nondegenerate polynomial of total degree 2 in x and y. The term non-degenerate means that $f(x, y)$ does not factor as a product of two linear polynomials (so that C is not the union of two lines). We say the conic C is *defined over* $\mathbb{Q}$ if $f(x, y)$ has coefficients in $\mathbb{Q}$.

The method we gave to find all rational points on the unit circle generalizes to all conics over $\mathbb{Q}$. If a conic C has one rational point P_0, then it has infinitely many rational points, and these points can be obtained by intersecting lines passing through P_0 with rational or infinite slope with C, just as we did in the case of the unit circle. The key here is that *C is defined by an equation of degree 2 with coefficients in $\mathbb{Q}$ and $P_0 = (x_0, y_0)$ is a rational point.* Given a line ℓ passing through P_0, when we substitute the equation of ℓ in the equation of C, we obtain *a quadratic equation with rational coefficients.* This equation has one root in $\mathbb{Q}$ corresponding to the point P_0. The other root will also have to be rational, leading to a rational point $P(\ell)$ on C. Varying the line ℓ, we obtain all the rational points on C.

We will illustrate this by some examples.

Example 12.2. (a) Find all rational points on the hyperbola

$$3x^2 - 2y^2 = 1,$$

if any such points exist.

[6] The terminology comes from the fact that these are the smooth curves one can get by intersecting a cone with planes.

(b) Use your answer to part (a) to give three primitive solutions to

$$3a^2 - 2b^2 = c^2$$

in the positive integers. (As in the case of Pythagorean triples, by a primitive solution here we mean a solution with $\gcd(a, b, c) = 1$.)

Solution. (a) Denote the hyperbola by C. Note that $P_0 = (1, 1)$ is a rational point on C. Let ℓ be a line passing through P_0, given by the equation

$$\ell : \ y - 1 = m(x - 1) \qquad (m = \text{slope of } \ell).$$

We find the intersections of ℓ with C. Substituting y from the equation of ℓ in the equation of C, we have

$$3x^2 - 2(mx - m + 1)^2 = 1,$$

which after expansion simplifies to

$$(3 - 2m^2)x^2 + 4m(m - 1)x - 2m^2 + 4m - 3 = 0.$$

We may assume $3 - 2m^2 \neq 0$, i.e., $m \neq \pm\sqrt{3/2}$, so that this is a quadratic equation (this excludes the two exceptional lines that only meet C once non-tangentially at P_0![7]). Since P_0 is a point of intersection of ℓ and C, one root to this quadratic equation is $x_0 = 1$. The product of the two roots is $(-2m^2 + 4m - 3)/(3 - 2m^2)$, hence the other root (= the x-coordinate of the point $P(\ell)$ in the figure) is

$$x_1 = \frac{-2m^2 + 4m - 3}{3 - 2m^2}.$$

Substituting $x = x_1$ in the equation of ℓ, we obtain that the second point of intersection of ℓ and C is the point

$$P(\ell) = \left(\frac{-2m^2 + 4m - 3}{3 - 2m^2}\ , \frac{2m^2 - 6m + 3}{3 - 2m^2}\right).$$

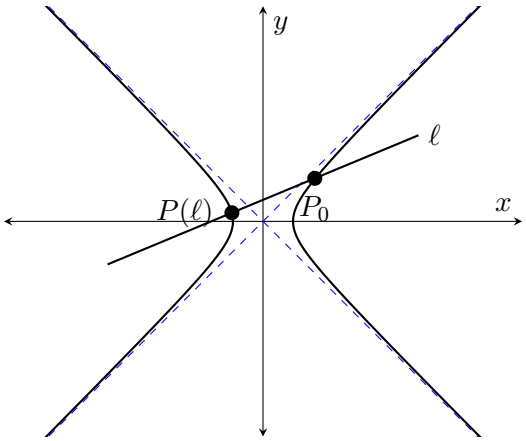
As in the case of the unit circle, if ℓ is the vertical line, the point $P(\ell)$ is obtained by letting $m \to \infty$ in the above formula.

Sending $\ell \mapsto P(\ell)$ we obtain a bijection between C and the collection of all the lines passing through P_0 with slope $\neq \pm\sqrt{3/2}$. This restricts to a bijection between the set $C(\mathbb{Q})$ of all the rational points of C and the set of all the lines passing through P_0 with rational or infinite slope. The point coming from the vertical line is $(1, -1)$ (use symmetry or let $m \to \infty$ in the formula for $P(\ell)$). We thus have

$$C(\mathbb{Q}) = \left\{\left(\frac{-2m^2 + 4m - 3}{3 - 2m^2}\ , \frac{2m^2 - 6m + 3}{3 - 2m^2}\right) : m \in \mathbb{Q}\right\} \cup \{(1, -1)\}.$$

(Since $\pm\sqrt{3/2}$ is not rational, those values of m are already excluded as we impose the rationality condition on m.)

[7] These are the two lines parallel to the asymptotes of C.



(b) Set $m = u/v$, where $u, v \in \mathbb{Z}$ are coprime and $v > 0$. After simplification we have

$$P(\ell) = (\frac{-2u^2 + 4uv - 3v^2}{3v^2 - 2u^2}\ , \frac{2u^2 - 6uv + 3v^2}{3v^2 - 2u^2}).$$

This is on C, so that

$$3(\frac{-2u^2 + 4uv - 3v^2}{3v^2 - 2u^2})^2 - 2(\frac{2u^2 - 6uv + 3v^2}{3v^2 - 2u^2})^2 = 1.$$

Multiplying through by $(3v^2 - 2u^2)^2$, we have

$$3(-2u^2 + 4uv - 3v^2)^2 - 2(2u^2 - 6uv + 3v^2)^2 = (3v^2 - 2u^2)^2.$$

Thus

$$(a, b, c) = (-2u^2 + 4uv - 3v^2, 2u^2 - 6uv + 3v^2, 3v^2 - 2u^2)$$

satisfies the equation $3a^2 - 2b^2 = c^2$. Taking

$$(u, v) = (0, 1),\ (1, 2),\ (1, 3)$$

we obtain the triples

$$(a, b, c) = (-3, 3, 3),\ (-6, 2, 10),\ (-17, 11, 25).$$

If $(X, Y, Z) = (a, b, c)$ satisfies the equation $3X^2 - 2Y^2 = Z^2$, then so do $(X, Y, Z) = (|a|, |b|, |c|)$ and $(X, Y, Z) = (a/d, b/d, c/d)$ for any nonzero d. Thus the three solutions above give us the three primitive solutions

$$(a, b, c) = (1, 1, 1),\ (3, 1, 5),\ (17, 11, 25)$$

in the positive integers. There are infinitely many primitive solutions in the positive integers. □

Example 12.3. (a) Find all rational points on the ellipse defined by

$$2x^2 + y^2 = 3,$$

if any such points exist.

(b) Use your answer to part (a) to give three primitive solutions to

$$2a^2 + b^2 = 3c^2$$

in the positive integers.

Solution. (a) The point $P_0 = (1, 1)$ is on the curve. Let ℓ be the line passing through P_0 with slope m, hence given by the equation $y = m(x-1)+1 = mx+(1-m)$. Substituting y from this in the equation of our ellipse $2x^2 + y^2 = 3$, after simplification we obtain

$$(2+m^2)x^2 + 2m(1-m)x + m^2 - 2m - 2 = 0.$$

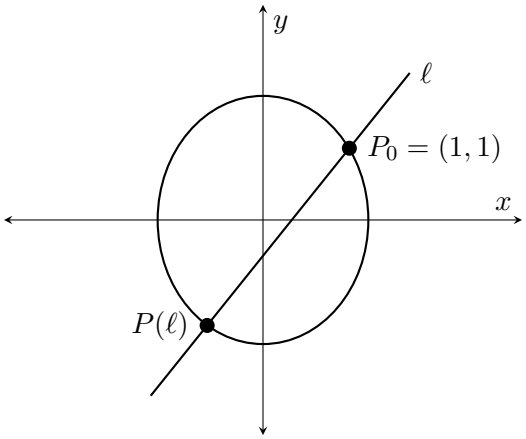
The roots of this are the x-coordinates of the points of intersection of ℓ and the ellipse. Since $P_0 = (1, 1)$ is an intersection point, $x = 1$ is a root. The product of the two roots is $(m^2 - 2m - 2)/(2 + m^2)$, so that the second root is $x = (m^2 - 2m - 2)/(2 + m^2)$. Denoting the second point of intersection by $P(\ell)$, after substituting its x-coordinate in the equation of ℓ to calculate its y-coordinate, we get

$$P(\ell) = (\frac{m^2 - 2m - 2}{2 + m^2}, \frac{-m^2 - 4m + 2}{2 + m^2}).$$

Sending $\ell \mapsto P(\ell)$ we obtain a bijection between the collection of lines ℓ passing through P_0 and the points on our ellipse. As before, $P(\ell)$ is a rational point if and only if m is rational or ℓ is the vertical line (with $m = \infty$). Thus here are all the rational points on our ellipse:

$$(\frac{m^2 - 2m - 2}{2 + m^2}, \frac{-m^2 - 4m + 2}{2 + m^2}) \quad (m \in \mathbb{Q})$$

together with $(1, -1)$ corresponding to the vertical line.



(b) Setting $m = u/v$ for u, v coprime integers with $v > 0$ in the formula for $P(\ell)$ we get the rational point

$$(\frac{u^2 - 2uv - 2v^2}{2v^2 + u^2}, \frac{-u^2 - 4uv + 2v^2}{2v^2 + u^2})$$

on the ellipse $2x^2 + y^2 = 3$, and hence the integral solution

$$(a, b, c) = (u^2 - 2uv - 2v^2,\ -u^2 - 4uv + 2v^2,\ 2v^2 + u^2)$$

to $2a^2 + b^2 = 3c^2$. Taking $(u, v) = (0, 1)$, $(1, 2)$ and $(3, 2)$, after replacing each (a, b, c) by $(|a/d|, |b/d|, |c/d|)$ with $d = \gcd(a, b, c)$ we obtain the three primitive solutions

$$(a, b, c) = (1, 1, 1),\ (11, 1, 9),\ (11, 25, 17).$$

to $2a^2 + b^2 = 3c^2$. □

We end this subsection by an example that illustrates that not every conic defined over $\mathbb{Q}$ has rational points.

Example 12.4. Find all rational points on the hyperbola C defined by

$$7x^2 - 4y^2 = 1,$$

if any such points exist.

Solution. We claim that the equation of C has no rational solutions (i.e., C has no rational points). Indeed, with a view towards getting a contradiction, suppose there exists a rational solution (x, y) to the equation. After taking a common denominator, we can write $x = a/c$ and $y = b/c$ for some $a, b, c, \in \mathbb{Z}$ with $c \neq 0$. Then we have

$$7(\frac{a}{c})^2 - 4(\frac{b}{c})^2 = 1 \quad \Rightarrow \quad 7a^2 - 4b^2 = c^2.$$

The equation on the right can be rewritten as

$$(2b)^2 + c^2 = 7a^2.$$

Since $c \neq 0$, the left hand side is positive and so $a \neq 0$, thus $7a^2$ is a positive integer. Note that the left hand side is a sum of two squares, so that $7a^2$ is a sum of two squares. But this is absurd, since the exponent of 7 (which is a prime congruent to 3 mod 4) in the prime factorization of $7a^2$ is odd and so by Theorem 10.7, $7a^2$ can not be a sum of two squares. □

Remark 12.5. (Not to be tested on) Let C be a smooth[8] plane curve defined by an equation

$$f(x, y) = 0,$$

where f is a polynomial of total degree d in x and y with rational coefficients. If $d = 2$, the curve C is a conic. As we saw, in this case the set of rational points of C is either empty or infinite.

If $d = 3$, then one can prove that depending on f, the set of rational points of C may be empty, finite but nonempty, or infinite. If this set is nonempty, the curve is an *elliptic curve* over $\mathbb{Q}$, and its set of rational points has some very nice extra structure described by the *Mordell-Weil theorem*. Elliptic curves are the subject of significant interest, due to the deep mathematics of them as well as applications in cryptography.

If $d > 3$, then the curve C will always have at most finitely many rational points. This was conjectured by Mordell in 1922 and proved by Faltings in 1983. Faltings was awarded the Fields Medal in 1986 mainly for this.

[8] Smooth in the "projective plane"