# Math 282 – Number Theory

Winter 2026 | Carleton College

**Deewang Bhamidipati**

**Acknowledgments**

*these notes are based on iterations of an upper-level Number Theory course at UC Santa Cruz first taught by Junecue Suh in Winter 2021, and by Deewang Bhamidipati in Summer and Fall 2021 based on Marty Weissman's* An Illustrated Theory of Numbers (first edition)

**(all errors introduced are my own)**

Last Updated: 16th December, 2025

# Contents


**0 Number Systems** **1**

**1 The Division Algorithm & Linear Diophantine Equations** **2**
1.1 Linear Diophantine Equations . . . 2
1.2 The Division Algorithm . . . 3
1.3 The Greatest Common Divisor . . . 4
1.4 Solving Linear Diophantine Equations . . . 6
Problems . . . 8

**2 Primes & Unique Factorisation** **11**
2.1 Fundamental Theorem of Arithmetic . . . 11
2.2 GCD & LCM via Factorisation . . . 12
2.3 Towards Arithmetic Functions . . . 13
2.4 Appreciating Uniqueness of Prime Factorisation . . . 15
2.5 Remarks on Distribution of Primes . . . 16
Problems . . . 17

**3 Arithmetic Functions I** **19**
3.1 Divisor-sum Functions . . . 19
3.2 Perfect Numbers & Mersenne Primes . . . 21
Problems . . . 23

**4 Rational Numbers** **25**
4.1 Fractions & Irrationality . . . 25
4.2 Algebraic Numbers . . . 26
4.3 Transcendental Numbers . . . 27
4.4 Diophantine Approximation & Ford Circles . . . 28
Problems . . . 36

**5 Towards Quadratic Diophantine Equations** **38**
5.1 Pythagorean Triples . . . 38
Problems . . . 41

**6 Modular Arithmetic** **43**
6.1 Congruence Modulo $m$ . . . 43
6.2 Solving Quadratic Diophantine Equations, so far . . . 46
6.3 Multiplicative Inverses Modulo $m$ . . . 47
Problems . . . 49

**7 Modular Dynamics** **52**
7.1 Additive Modular Dynamics . . . 52
7.2 Units Modulo $m$ . . . 53
7.3 Multiplicative Modular Dynamics . . . 54
7.4 Primality Testing . . . 56
Problems . . . 57

**8 Arithmetic Functions II** **59**
8.1 Euler-Totient Function . . . 59
8.2 Discrete Convolution . . . 60
Problems . . . 61

**9 Primitive Roots & Polynomials Modulo $p$** **64**
9.1 Primitive Roots Modulo $p$ . . . 64
9.2 Polynomials Modulo $p$ . . . 64
9.3 Proof of Primitive Root Theorem . . . 69

9.4 Cryptographic Application: Diffie-Helman Key Exchange . . . 71
Problems . . . 71

**10 Assembling the Modular World** **73**
10.1 The Chinese Remainder Theorem . . . 73
10.2 Applying CRT . . . 75
Problems . . . 77

**11 Quadratic Reciprocity** **78**
11.1 Quadratic Residues . . . 78
11.2 The Idea of Partnership . . . 78
11.3 Towards Quadratic Reciprocity . . . 80
11.4 Legendre Symbol & Quadratic Reciprocity . . . 82
11.5 Application: Fermat's Christmas Theorem . . . 89
Problems . . . 95

**12 Proof of Quadratic Reciprocity à la Zolotarev** **97**
12.1 Permutations & their Sign . . . 97
12.2 Permutations and Quadratic Reciprocity . . . 103
Problems . . . 107

**13 Proof of Quadratic Reciprocity à la Eisenstein following Gauss** **108**

# 0. Number Systems

The fundamental system of numbers we consider in number theory is the **integers**, denoted

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$ ("Z" stands for *zahlen*, the word for number in German)

More generally, for any integer $b$ we denote $\mathbb{Z}_{\geqslant b} = \{b,\ b+1,\ b+2,\ \ldots\}$.

In particular, we denote $\mathbb{Z}_{\geqslant 1} = \{1, 2, \ldots\}$, the set of positive integers, as $\mathbb{Z}_+$.

The set of non-negative integers $\mathbb{Z}_{\geqslant 0}$ is denoted as $\mathbb{N} = \{0, 1, 2, \ldots\}$ and referred to as the set of **natural numbers**. We choose to include 0 in $\mathbb{N}$, while some authors do not. This way, $\mathbb{N}$ contains a neutral element for both operations (0 for addition, 1 for multiplication).

We also would like a number system where dividing by integers always makes sense and is not too large; this is the **rational numbers**, denoted

$$\mathbb{Q} = \left\{\frac{a}{b}\ :\ a, b \in \mathbb{Z},\ b \neq 0\right\}$$ ("Q" stands for *quotient*)

A bigger number system where division always makes sense is the **real numbers**, denoted as $\mathbb{R}$.

$\mathbb{R}$ consists of those numbers with a decimal representation. $\mathbb{R}$ is made up of $\mathbb{Q}$ and the set of, so-called, irrational numbers. Even amongst irrational numbers, we can make a distinction: numbers such as $\sqrt{2}$ that are solutions to polynomial equations ($x^2 - 2 = 0$) and numbers like $\pi$ which are not. The former are called **algebraic numbers** and much of field and Galois theory can be used to study them carefully, the latter are called **transcendental numbers**.

$\mathbb{R}$ is just one of many " analytic jumps" one can make from $\mathbb{Q}$, there are more (indexed by prime numbers), that are treated in advanced number theory, called the $p$-adic numbers, denoted $\mathbb{Q}_p$.

Our final number system is the one where we can imagine all numbers we wish to understand sit, the **complex numbers**, denoted

$$\mathbb{C} = \left\{a + bi\ :\ a, b \in \mathbb{R},\ i^2 = -1\right\}$$

$\mathbb{C}$ is an "algebraic jump" from $\mathbb{R}$ since $i$ is a solution to a polynomial equation with rational coefficients

$$x^2 + 1 = 0.$$

We have the hierarchy: $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

## Questions in Number Theory

Number Theory, more than any other field in mathematics, is defined by the questions it entails; more often than this subject is context. The kinds of questions one asks are as follows:

- **Involving polynomial equations**
  - Does the polynomial equation $2x - 1 = 0$ have an integer solution?
    *Ans.* No, this is equivalent to $1/2 \notin \mathbb{Z}$.
  - Does the polynomial equation $x^2 + y^2 = 1$ have a rational solution?
    *Ans.* Yes, this is related to a discussion on Pythagorean triplets and the unit circle.
  - Elliptic Curve Cryptography is an application of number theory resulting from this line of question.
- **Involving prime numbers**
  - Counting prime numbers – A result of paramount importance here is the *Prime Number Theorem*.
  - On the application front, the RSA cryptosystem is of this nature.
- **Involving geometry:** e.g., can you "square a circle", i.e., can there be a square whose area is $\pi$?
  *Ans.* No! This is related to the notion of transcendence and constructibility.

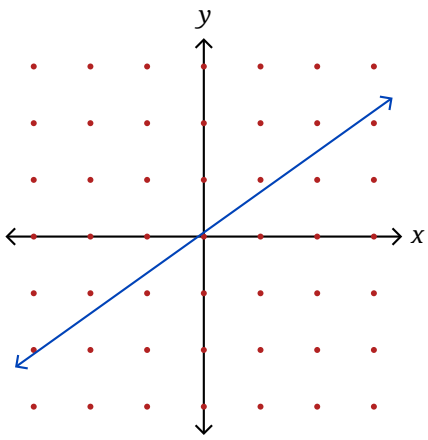
# 1. The Division Algorithm & Linear Diophantine Equations

## 1.1. Linear Diophantine Equations

Let us pose the following geometric question:

In the plane, consider the integer grid and a line with rational slope and rational $y$-intercept.

*When does it intersect the integer grid? If it intersects, at how many points does it intersect?*




Algebraically, we may write the equation of the line as $AX + BY = C$ for some $A, B, C \in \mathbb{Z}$, and we are asking if there exist $(x, y) \in \mathbb{Z}^2$ such that

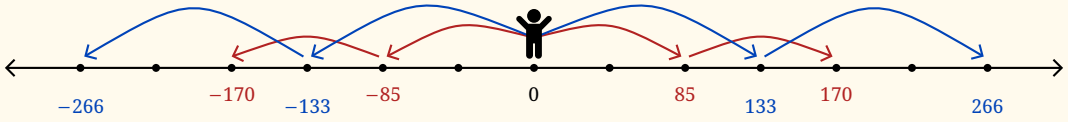
$$Ax + By = C$$

Furthermore, we are also asking if we can find one such $(x, y) \in \mathbb{Z}^2$, can we find all?

**Question.** *Can we find $(x, y) \in \mathbb{Z}^2$ such that $133x + 85y = 1$?*

**Discussion.** Visually, we are asking: suppose you start at 0 on the number line and you're allowed to

1. **hop** 133 steps left (-133) or right (+133)
2. **skip** 85 steps left (-85) or right (+85)




Then we want to know if you can hop $x$-many times and skip $y$-many times to get to 1. For example, hopping twice to the right and skipping thrice to the left gets you

$$133 \cdot (+2) + 85 \cdot (-3) = 266 - 255 = 11$$

The answer is **yes**. The theoretical reason is the gcd, *greatest common divisor*, and the algorithmic reason is the *(Euclidean) Division Algorithm*.

This first requires the *Division lemma*.

**Lemma 1.1** (The Division Lemma)**.** *Given two integers $a, b$ with $b \neq 0$, there exist unique integers $q$ and $r$ such that*

$$a = bq + r, \qquad 0 \leqslant r < |b|$$

*where $q$ is the* **quotient** *and $r$ is the* **remainder**.

Applying Lemma 1.1 to any integer $a = n$ and $b = 2$ gives us $n = 2q + r$ for $0 \leqslant r < 2$; equivalently, $r = 0$ or 1.

If $r = 0$, then $n = 2q$, and $n$ is said to be **even**. If $r = 1$, then $n = 2q + 1$, and $n$ is said to be **odd**.

**Definition 1.2** (Parity)**.** The **parity** of an integer $n$ is its property to be either even or odd.

## 1.2. The Division Algorithm

**Definition 1.3** (The Division Algorithm)**.** Start with positive integers $a, b$, assume $a \geqslant b$.

- Divide $a$ by $b$, i.e., apply the division lemma (Lemma 1.1): $a = bq + r$ for unique integers $q$ and $0 \leqslant r < b$.
- If $r = 0$, *halt*. If not, repeat the previous steps by replacing $(a, b)$ by $(b, r)$.
- Continue until your remainder is 0, this process will terminate in finite steps (due to the **well-ordering principle**).

Let us revisit the equation from above

$$133X + 85Y = 1$$

We will see how the algorithm above makes it possible for us to find a required solution.

**Example 1.4.** Employ the Division Algorithm to $(133, 85)$ and find a solution to the equation $133X + 85Y = 1$.

*Answer.* Let us employ the Division Algorithm

$$133 = 85 \cdot (1) + 48 \tag{1}$$
$$85 = 48 \cdot (1) + 37 \tag{2}$$
$$48 = 37 \cdot (1) + 11 \tag{3}$$
$$37 = 11 \cdot (3) + 4 \tag{4}$$
$$11 = 4 \cdot (2) + 3 \tag{5}$$
$$4 = 3 \cdot (1) + 1 \tag{6}$$
$$3 = 1 \cdot (3) + 0 \tag{7}$$

Let us take the last non-zero remainder, 1, and work backwards in the following fashion:

$$\begin{aligned}
1 &= 4 + 3 \cdot (-1) && \text{from (6)} \\
&= 4 + (11 - 4 \cdot (2)) \cdot (-1) && \text{using (5)} \\
&= 11 \cdot (-1) + 4 \cdot (3) && \textit{rearranging} \\
&= 11 \cdot (-1) + (37 - 11 \cdot (3)) \cdot (3) && \text{using (4)} \\
&= 37 \cdot (3) + 11 \cdot (-10) && \textit{rearranging} \\
&= 37 \cdot (3) + (48 - 37 \cdot (1)) \cdot (-10) && \text{using (3)} \\
&= 48 \cdot (-10) + 37 \cdot (13) && \textit{rearranging} \\
&= 48 \cdot (-10) + (85 - 48 \cdot (1)) \cdot (13) && \text{using (2)} \\
&= 85 \cdot (13) + 48 \cdot (-23) && \textit{rearranging} \\
&= 85 \cdot (13) + (133 - 85 \cdot (1)) \cdot (-23) && \text{using (1)} \\
&= 133 \cdot (-23) + 85 \cdot (36) && \textit{rearranging}
\end{aligned}$$

Therefore $(x, y) = (-23, 36)$ is such that $133x + 85y = -3059 + 3060 = 1$.

**Example 1.5.** Does there exist a solution to the equation $91X + 49Y = 1$.

*Answer.* Let us employ the Division Algorithm as we did in the previous example

$$91 = 49 \cdot (1) + 42$$

$$49 = 42 \cdot (1) + 7$$

$$42 = 7 \cdot (6) + 0$$

Unlike the previous example where the last non-zero remainder was exactly the number on the right hand side of the given equation, we have 7 which is not the number on the right hand side of the given equation, 1. So, one may guess that this equation doesn't have a solution.

One would then be correct, let us show this by way of contradiction. Suppose there did exist a pair $(x, y) \in \mathbb{Z}^2$ such that $91x + 49y = 1$, which gives us

$$7 \cdot (13x + 7y) = 1.$$

This tells us that $7 \mid 1$ (7 divides 1), which is preposterous. Therefore no solution exists. ☝

It would have been a different story if the right hand side was divisible by 7, which happens to be $\gcd(91, 49)$ and the last non-zero remainder we obtained using the division algorithm. This is not a coincidence.

**Remark 1.6.** The fact that the equation $133X + 85Y = 1$ has a solution $(x, y) = (-23, 36)$ means that $133x + 85y = C$ has a solution for any integer $C$, which is nothing but $(xC, yC) = (-23C, 36C)$

$$133(-23C) + 85(36C) = C \cdot (133(-23) + 85(36)) = C \cdot 1 = C$$

## 1.3. The Greatest Common Divisor

**Definition 1.7** (Greatest Common Divisor)**.** Let $a, b$ be non-zero integers, than any *positive integer* $g$ is called a **greatest common divisor** of $a$ and $b$, denoted $\gcd(a, b)$ or $\gcd(b, a)$, if

(D1) $g \mid a$ and $g \mid b$; and (a *common divisor*)

(D2) $d$ is any integer such that $d \mid a$ and $d \mid b$, then $d \mid g$ (a *largest* common divisor)

**Example 1.8.** Consider integers $-4,\ b = 6$

divisors of $-4$ are: $-1, 1, -2, 2, -4, 4$ divisors of 6 are: $-1, 1, -2, 2, -3, 3, -6, 6$

One immediately sees that 2 satisfies both (D1) and (D2) for $a = -4$ and $b = 6$ and therefore $\gcd(-4, 6) = 2$.

Similarly, we see that $\gcd(91, 49) = 7,\ \gcd(133, 85) = 1$

**Lemma 1.9.** *The* gcd *for a given pair of non-zero integers is unique.*

*Proof.* Let $a, b$ be non-zero integers and suppose $g$ and $g'$ are two gcd's of $a$ and $b$. In particular, both of them are common divisors of $a$ and $b$, therefore by (D2) we have $g \mid g'$ and $g' \mid g$. Hence $g = g'$, since $g, g' > 0$; see Problem 1.2 (v). Thus, the gcd is unique. □

**Theorem 1.10.** *Let $a, b$ be positive integers. The last non-zero remainder $R$ obtained under the Division Algorithm applied to $a$ and $b$ is equal to* $\gcd(a, b)$.

*Proof.* To prove this theorem, we will first prove the following lemma

> **Lemma 1.11.** *Let $u, v, q, r$ be integers such that $u = vq + r$, then*
>
> $$g = \gcd(u, v) \quad \textit{if and only if} \quad g = \gcd(v, r)$$

*Proof.* ($\Rightarrow$) Suppose $g = \gcd(u, v)$, let us prove $g = \gcd(v, r)$.

(D1) Since $g = \gcd(u, v)$, therefore $g \mid u$ and $g \mid v$. Since $u = vq + r$, hence $r = u - vq$ and thus $g \mid r$; see Problem 1.2 (iv). Therefore $g \mid v$ and $g \mid r$.

(D2) Let $d \mid v$ and $d \mid r$, then since $u = vq + r$, we have $d \mid u$. That is, $d \mid u$ and $\mid v$, and since $g = \gcd(u, v)$, by definition $g \mid d$.

By definition, we then have $g = \gcd(v, r)$.

A very similar argument gives you ($\Leftarrow$). □

With this lemma in hand, let us assume, without loss of generality, $a \geqslant b$. We employ the Division Algorithm and let us assume it terminates in $n$ steps, that is our algorithm gives us the following

$$\begin{aligned}
a &= bq_1 + r_1 && \text{STEP 1}\\
b &= r_1q_2 + r_2 && \text{STEP 2}\\
r_1 &= r_2q_3 + r_3 && \text{STEP 3}\\
&\vdots\\
r_{n-4} &= r_{n-3}q_{n-2} + r_{n-2} && \text{STEP } n-2\\
r_{n-3} &= r_{n-2}q_{n-1} + R && \text{STEP } n-1\\
r_{n-2} &= Rq_n + 0 && \text{STEP } n
\end{aligned}$$

Observe that in STEP $n$ we have obtained $R \mid r_{n-2}$. Our Lemma 1.11 tells us that

$$\begin{aligned}
\gcd(a, b) &= \gcd(b, r_1) && \text{from STEP 1}\\
&= \gcd(r_1, r_2) && \text{from STEP 2}\\
&\vdots\\
&= \gcd(r_{n-3}, r_{n-2})\\
&= \gcd(r_{n-2}, R) && \text{from STEP } n-1\\
&= R && \text{since } R \mid r_{n-2} \text{ and Problem 1.3 (ii)}
\end{aligned}$$

Hence $R = \gcd(a, b)$, as needed to be shown. □

**Example 1.12** (in-class)**.** Consider the pair $(39, 14)$, using the Division Algorithm determine $\gcd(39, 14)$ and find a solution to $39X + 14Y = \gcd(39, 14)$.

We distil the above theorem and the Division Algorithm into the following major theorem.

**Theorem 1.13** (Bézout's Identity)**.** *Given non-zero integers $a, b$, there exist integers $x, y$ such that*

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

*Proof.* Theorem 1.10 and the Division Algorithm applied backwards, as in Example 1.4, gives us $x, y \in \mathbb{Z}$ such that

$$|a|x + |b|y = \gcd(a, b)$$

- CASE I: If $a, b > 0$, then $(x, y)$ is the pair we want.
- CASE II: If $a > 0, b < 0$, then $(x, -y)$ is the pair we want.
- CASE III: If $a < 0, b > 0$, then $(-x, y)$ is the pair we want.
- CASE IV: If $a, b < 0$, then $(-x, -y)$ is the pair we want. □

## 1.4. Solving Linear Diophantine Equations

We are concerned with finding solutions to the equation

$$AX + BY = C \tag{❀}$$

where $A, B, C \in \mathbb{Z}$ and $A, B \neq 0$.

**Theorem 1.14** (Existence of a Solution)**.** (❀) *has a solution if and only if* $g := \gcd(A, B) \mid C$.

*Proof.* ($\Rightarrow$) Suppose there exists a solution $(x, y) \in \mathbb{Z}^2$ such that

$$Ax + By = C.$$

Since $g = \gcd(A, B)$, then $g \mid A$ and $g \mid B$, therefore $g \mid (Ax + By) = C$.

($\Leftarrow$) Let $g \mid C$, then $C = gD$ for some integer $D$. By Bézout's Identity, there exist integers $x_0$, $y_0$ such that

$$Ax_0 + By_0 = g, \quad \text{then } C = gD = A(x_0D) + B(y_0D).$$

Therefore $(x, y) = (x_0D, y_0D)$ solves (❀). □

**Example 1.15.** Find $x, y \in \mathbb{Z}$ that solves $27x + 105y = 81$.

*Answer.* We first employ the Division Algorithm to compute $\gcd(27, 105)$

$$\begin{aligned} 105 &= 27 \cdot (3) + 24 \\ 27 &= 24 \cdot (1) + 3 \\ 24 &= 3 \cdot (8) + 0 \end{aligned}$$

By Theorem 1.10, $\gcd(27, 105) = 3$, and since $3 \mid 81$, therefore the given equation has a solution. We now work the above calculation backwards

$$\begin{aligned} 3 &= 27 - 24 \cdot (1) \\ &= 27 - (105 - 27 \cdot (3)) = 27 \cdot (4) + 105 \cdot (-1) \end{aligned}$$

Hence

$$81 = 27 \cdot 3 = 27 \cdot (27 \cdot 4) + 105 \cdot (27 \cdot (-1)) = 27 \cdot (108) + 105 \cdot (-27)$$

Thus $(x, y) = (108, -27)$ solves the given equation. 👌

**Definition 1.16** (Least Common Multiple)**.** Let $a, b$ be non-zero integers, than any *positive integer* $\ell$ is called a **least common multiple** of $a$ and $b$, denoted $\operatorname{lcm}(a, b)$ or $\operatorname{lcm}(b, a)$, if

(L1) $a \mid \ell$ and $b \mid \ell$; and (a *common multiple*)

(L2) $m$ is any integer such that $a \mid m$ and $b \mid m$, then $\ell \mid m$ (a *smallest* common multiple)

**Example 1.17.** Consider integers $-4$, $b = 6$

multiples of $-4$ are: $\pm 4, \pm 8, \pm 12, \pm 16, \ldots$ divisors of 6 are: $\pm 6, \pm 12, \pm 18, \ldots$

One immediately sees that 12 satisfies both (L1) and (L2) for $a = -4$ and $b = 6$ and therefore $\operatorname{lcm}(-4, 6) = 12$.

Similarly, we see that $\operatorname{lcm}(91, 49) = 637$.

Our immediate next **goal** is to compute the set of *all* solutions to the equation

$$AX + BY = C \tag{$\clubsuit$}$$

provided $\gcd(A, B) \mid C$, since otherwise the equation has no solutions.

Our previous discussions tell us that we know how to find $(x_0, y_0) \in \mathbb{Z}^2$ such that

$$Ax_0 + By_0 = C \tag{$\spadesuit_1$}$$

Suppose $(x_1, y_1)$ is another solution, that is

$$Ax_1 + By_1 = C \tag{$\spadesuit_2$}$$

Then subtracting ($\spadesuit_1$) from ($\spadesuit_2$) gives us

$$Ax' + By' = 0 \tag{$\heartsuit$}$$

where $x' = x_1 - x_0$ and $y' = y_1 - y_0$.

**Proposition 1.18.** *Let $A, B \in \mathbb{Z}$.*

(i) *For any $n \in \mathbb{Z}$, let*

$$x' = n \cdot \frac{\operatorname{lcm}(A, B)}{A} \quad \text{and} \quad y' = -n \cdot \frac{\operatorname{lcm}(A, B)}{B}.$$

*Then $Ax' + By' = 0$, that is $(x', y') \in \mathbb{Z}^2$ solves ($\heartsuit$)*

(ii) *All integer solutions to ($\heartsuit$) are of the form given in* (i).

*Proof.* For the given $(x', y')$ we clearly have

$$Ax' + By' = A\left(n \cdot \frac{\operatorname{lcm}(A, B)}{A}\right) + B\left(-n \cdot \frac{\operatorname{lcm}(A, B)}{B}\right) = 0,$$

thus proving (i).

Suppose $x'', y'' \in \mathbb{Z}$ were solutions to ($\heartsuit$), that is $Ax'' + By'' = 0$. Let

$$m \coloneqq Ax'' = B(-y''),$$

then $A \mid m$ and $B \mid m$. By definition, $\operatorname{lcm}(A, B) \mid m$, therefore $m = n' \cdot \operatorname{lcm}(A, B)$ for some integer $n'$. Giving us

$$Ax'' = m = n' \cdot \operatorname{lcm}(A, B) \qquad B(-y'') = m = n' \cdot \operatorname{lcm}(A, B)$$

Therefore

$$x'' = n' \cdot \frac{\operatorname{lcm}(A, B)}{A} \qquad y'' = -n' \cdot \frac{\operatorname{lcm}(A, B)}{B};$$

hence (ii) is proved. □

**Theorem 1.19** (Algorithm to Solve ($\clubsuit$))**.**

1. *Compute $\gcd(A, B)$ using the Division Algorithm.*
2. *If $\gcd(A, B) \nmid C$, there exists no solution.*
3. *If $\gcd(A, B) \mid C$, then let $g = \gcd(A, B)$ and $C = gD$*
   (i) *Use the Division Algorithm on $A, B$, and work backwards to find $(x_0', y_0') \in \mathbb{Z}^2$ such that $Ax_0' + By_0' = g$.*
   (ii) *Then $(x_0, y_0) = (x_0'D, y_0'D)$ is a particular solution to $Ax + By = C$*

(iii) *The general solution will then be*

$$\begin{cases} x = x_0 + n \cdot \dfrac{\mathrm{lcm}(A,B)}{A} \\ y = y_0 - n \cdot \dfrac{\mathrm{lcm}(A,B)}{B} \end{cases}$$

*for any $n \in \mathbb{Z}$. For a given integer $n$, let the corresponding solution be $(x_n, y_n)$.*

*Proof.* The only thing we need to prove is (iii). Let $(x', y')$ be any other solution to (✻), i.e. $Ax' + By' = C$. Then

$$Ax'' + By'' = 0,$$

where $x'' = x' - x_0$ and $y'' = y' - y_0$. Therefore

$$x'' = n \cdot \frac{\mathrm{lcm}(A,B)}{A} \quad \text{and} \quad y'' = -n \cdot \frac{\mathrm{lcm}(A,B)}{B}$$

by Proposition 1.18. Hence

$$x' = x_0 + n \cdot \frac{\mathrm{lcm}(A,B)}{A} \quad \text{and} \quad y' = y_0 - n \cdot \frac{\mathrm{lcm}(A,B)}{B}$$

and thus we have proved (iii). □

**Example 1.20.** Find all solutions to the equation $27X + 105Y = 81$.

*Answer.* We have found a particular solution $(x_0, y_0) = (108, -27)$ to the given equation in Example 1.15. Further, we can calculate the lcm as follows (we will prove this later in Lemma 2.7)

$$\mathrm{lcm}(27, 105) = \frac{27 \cdot 105}{\gcd(27, 105)} = \frac{27 \cdot 105}{3} = 945.$$

Therefore, the general solution is

$$x = 108 + n \cdot \frac{945}{27} = 108 + 35n, \qquad y = -27 - n \cdot \frac{945}{105} = -27 - 9n$$

That is, the set of all solutions to the given equation is $\{(108 + 35n, -27 - 9n) \ : \ n \in \mathbb{Z}\}$ ☝

**Example 1.21** (in-class)**.** Find all solutions to the equation $117X + 42Y = 33$.

## Problems

**Problem 1.1.** In this problem we will work out a proof of Lemma 1.1.

Let $a$ and $b \neq 0$ be integers. We wish to prove that there exist unique integers $q$ and $r$ such that $0 \leqslant r < |b|$ and

$$a = bq + r$$

We first prove existence of $q$ and $r$.

(a) Define

$$q = \begin{cases} +\left\lfloor \dfrac{a}{|b|} \right\rfloor & \text{if } b > 0 \\ -\left\lfloor \dfrac{a}{|b|} \right\rfloor & \text{if } b < 0 \end{cases}$$

where $\lfloor x \rfloor$ is the largest integer $\leqslant x$. Define $r = a - bq$ and prove $0 \leqslant r < |b|$.

We now prove the uniqueness of $q$ and $r$.

(b) Assume you had

$$a = bq_1 + r_1$$
$$a = bq_2 + r_2$$

for integers $q_1, q_2, r_1, r_2$ with $0 \leqslant r_1, r_2 < |\, b \,|$

Dividing the equations by $|\, b \,|$ and using the fact that $\lfloor x \rfloor = 0$ for a number $0 \leqslant x < 1$, first prove that $q_1 = q_2$. Then conclude $r_1 = r_2$.

**Problem 1.2** (Divisibility)**.** Consider integers $x$, $y$, we say that

$x$ **divides** $y$ (or) $y$ is a **divisor** of $x$, denoted $x \mid y$, if *there exists an integer $u$ such that* $y = xu$

Let $a, b, c$ be integers, then show that

(i) if $a \mid b$ and $b \neq 0$, then $|a| \leqslant |b|$.

(ii) if $a \mid b$, then $a \mid bc$.

(iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.

(iv) if $c \mid a$ and $c \mid b$, then $c \mid (am + bn)$ for any integer $m$ and $n$.

(v) if $a \mid b$ and $b \mid a$, then $a = \pm b$.

(vi) if $c \neq 0$, then $a \mid b$ if and only if $ac \mid bc$.

**Problem 1.3.** Let $a, b$ be non-zero integers. Prove that

(i) $\gcd(a, 0) = |a|$; $\gcd(a, 1) = 1$.

(ii) if $b \mid a$, then $\gcd(a, b) = |\, b \,|$.

(iii) $\gcd(a, a + 1) = 1$;

(iv) $\gcd(a, b) = \gcd(|a|, |b|)$.

(v) $\gcd(ka, kb) = |k| \gcd(a, b)$, for all $k \in \mathbb{Z}$.

(vi) if $\gcd(a, k) = \gcd(b, k) = 1$, then $\gcd(ab, k) = 1$, for all $k \in \mathbb{N}$.

(vii) if $\gcd(a, b) = 1$, then $\gcd(a^m, b^n) = 1$, for all $m, n \in \mathbb{N}$.

**Problem 1.4.** Let $a, b, c$ be integers, and let $g \coloneqq \gcd(a, \gcd(b, c))$.

(i) Prove that $g$ satisfies the following properties

(P1) $g \mid a$, $g \mid b$ and $g \mid c$, i.e., $g$ is a common divisor of $a, b$ and $c$

(P2) If $d$ is a common divisor of $a, b$ and $c$, then $d \mid g$.

(ii) Show that $g = \gcd(b, \gcd(a, c)) = \gcd(c, \gcd(a, b))$

For this reason, we will write $\gcd(a, b, c) \coloneqq \gcd(a, \gcd(b, c))$, and call it *the* greatest common divisor of $a, b$ and $c$.

**Problem 1.5.** Using Problem 1.4 define $\gcd(a_1, \ldots, a_n)$ for integers $a_1, \ldots, a_n$, where $n \geqslant 4$.

**Problem 1.6.** Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a, b) = d$, then prove that $a \mid dc$.

Hint. Bezout's identity.

**Problem 1.7.** Let $a, b, c \in \mathbb{Z}$. If $a \mid c,\ b \mid c$ and $\gcd(a, b) = 1$, then prove that $ab \mid c$.

Hint. Bezout's identity.

**Problem 1.8.** Let $a, b, c \in \mathbb{Z}$. Prove that $\gcd(a, b) = 1$ if and only if $\gcd(a^2, b^2) = 1$.

Hint. For the forward direction, try cubing the expression you get from Bezout's identity.

**Problem 1.9.** Let $a, b \in \mathbb{Z}$. Then prove that if $g = \gcd(a, b)$, then $\gcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1$.

**Problem 1.10.**

(i) Using the Division Algorithm, find a particular solution $(x, y)$ to the equation $150x + 111y = 15$.

(ii) Proceed to find all the integer solutions to the equation $150x + 111y = 15$.

(iii) Find all the integer solutions $(x, y)$ to the equation $-187x + 68y = 288$. (If none exists, prove it.)

**Problem 1.11.** Look at Problem 1.4, write and prove the statements analogous for the lcm.

**Problem 1.12.**

(i) Prove that there exists no integer solution $(x, y, z)$ to the equation

$$18x - 27y + 39z = 4.$$

(ii) Find *an* integer solution $(x, y, z)$ to the equation

$$18x - 27y + 39z = 6.$$

(iii) **(challenge)** Find *all* integer solutions $(x, y, z)$ to the equation $18x - 27y + 39z = 6$.

Your answer should give explicit formulae for $x, y, z$ in terms of two independent integer parameters $m,\ n$.

(not unlike the case of two variables where we have one independent integer parameter, as seen in Proposition 1.18 and Theorem 1.19).

# 2. Primes & Unique Factorisation

**Definition 2.1** (Prime & Composite)**.** Let $n > 0$ be an integer.

- $n$ is **prime** (or a **prime number**) if $n > 1$ and 1 and itself are its only divisors.
- $n$ is **composite** if $n > 1$ and is not a prime; equivalently, $n = ab$ for some integers $1 < a, b < n$.
- $n = 1$ is called a unit.

**Definition 2.2** (Coprime)**.** We say integers $a,\ b$ are **coprime** (or **relatively/mutually prime**) if $\gcd(a, b) = 1$.

## 2.1. Fundamental Theorem of Arithmetic

**Lemma 2.3.** *Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

*Proof.* Since $\gcd(a, b) = 1$, by Bézout's Identity, there exist integers $x, y$ such that

$$1 = ax + by, \qquad \text{therefore} \quad c = acx + bcy$$

Clearly $a \mid ac$ and, by assumption, $a \mid bc$, hence $a \mid c$. □

**Corollary 2.4** (Characterisation of Primes)**.** *Let $p$ be a prime number and $b, c \in \mathbb{Z}$. If $p \mid bc$, then $p \mid b$ or $p \mid c$.*

*Proof.* Suppose $p \mid b$, then we have nothing to prove.

So assume that $p \nmid b$, and consider $g := \gcd(p, b)$. Necessarily, $g \mid p$ and therefore $g = 1$ or $g = p$. If $g = p$, then since $g \mid b$, we have $p \mid b$, contradicting our assumption; hence $g = 1$. Thus, by Lemma 2.3 we get $p \mid c$. □

**Theorem 2.5** (Fundamental Theorem of Arithmetic a.k.a. Unique Prime Factorisation)**.** *Let $n > 0$ be an integer.*

1. (EXISTENCE) *$n$ admits a prime factorisation, i.e. there exist integers $e_p \geqslant 0$ for each prime $p$ such that*
   - *$e_p = 0$, for all $p > n$*
   - *$n = 2^{e_2} \cdot 3^{e_3} \cdots p^{e_p} \cdots$*
2. (UNIQUENESS) *Suppose $n$ admits another prime factorisation, say $n = 2^{f_2} \cdot 3^{f_3} \cdots p^{f_p} \cdots$. Then, we have*

$$e_p = f_p, \quad \text{for every prime } p.$$

*In particular, $n$ has a prime factor.*

*Proof* (skipped in class)*.* We prove existence of prime factorization by inducting on $n$. For $n = 1$ and $n = 2$, we note

$$1 = 2^{e_2}\, 3^{e_3} \cdots p^{e_p} \cdots, \quad \text{where } e_p = 0 \text{ for every prime } p$$
$$2 = 2^{e_2}\, 3^{e_3} \cdots p^{e_p} \cdots, \quad \text{where } e_2 = 1 \text{ and } e_p = 0 \text{ for every prime } p > 2$$

Hence the existence statement holds true for $n = 1$ and $n = 2$. Assume that the existence statement is true for every positive integer $< n$.

Consider $n$. If $n$ is prime, then

$$n = 2^{e_2}\, 3^{e_3} \cdots n^{e_n} \cdots p^{e_p} \cdots, \quad \text{where } e_n = 1 \text{ and } e_p = 0 \text{ for every prime } p \neq n;$$

in particular $e_p = 0$ for any prime $p > n$, so the existence statement holds.

Now, suppose that if $n$ was composite instead, then necessarily $n = ab$ for integers $1 < a, b < n$.

By the inductive hypothesis, both $a$ and $b$ possess prime factorisations, say

$$a = 2^{i_2}\, 3^{i_3} \cdots q^{i_q} \cdots \qquad \text{and} \qquad b = 2^{j_2}\, 3^{j_3} \cdots r^{j_p} \cdots ,$$

where the exponents are positive integers, and $i_q = j_r = 0$ for every prime $q > a$ and $r > b$, in particular $i_p = j_p = 0$ for every prime $p > n$ since $n > a, b$. Therefore,

$$n = ab = 2^{i_2+j_2}\, 3^{i_3+j_3} \cdots p^{i_p+j_p} \cdots ,$$

where the exponents are again, necessarily, positive integers and we have $i_p + j_p = 0$ for every prime $p > n$. Hence, the existence statement is true for $n$.

Therefore, by the principal of mathematical induction, the existence statement is true for every integer $n$.

Let us now prove the uniqueness statement, suppose an integer $n > 0$ possesses the following prime factorizations

$$n = 2^{e_2}\, 3^{e_3} \cdots p^{e_p} \cdots = 2^{f_2}\, 3^{f_3} \cdots p^{f_p} \cdots ,$$

where the exponents satisfy the properties in the existence statement.

For the sake of contradiction, suppose that there exists a prime $q$ such that $e_q \neq f_q$. Let us assume, without loss of generality, that $e_q < f_q$. Define $d_q = f_q - e_q > 0$, and consider

$$\frac{n}{e_q} = 2^{e_2}\, 3^{e_3} \cdots q^0 \cdots = 2^{f_2}\, 3^{f_3} \cdots q^{d_q} \cdots .$$

Observe that $q$ divides the latter expression since $d_q > 0$, so it should divide the former expression. But since the exponent of $q$ is 0 in the former expression, $q$ necessarily does not divide it. Hence we have arrived at a contradiction. Thus $e_p = f_p$ for every prime $p$ and the uniqueness statement follows. □

**Proposition 2.6.** *Let $a, b$ be positive integers with the following prime factorisation*

$$a = 2^{e_2} 3^{e_3} \cdots p^{e_p} \cdots , \quad b = 2^{f_2} 3^{f_3} \cdots p^{f_p} \cdots$$

*Then $a \mid b$ if and only if $e_p \leqslant f_p$, for every prime $p$.*

*Proof.* ($\Rightarrow$) Suppose $a \mid b$, then $b = ac$ for some positive integer $c$. Let $c = 2^{d_2} 3^{d_3} \cdots p^{d_p} \cdots$, then

$$b = ac = 2^{e_2+d_2} 3^{e_3+d_3} \cdots p^{e_p+d_p} \cdots$$

By uniqueness of prime factorisation we have $f_p = e_p + d_p \geqslant e_p$ for every prime $p$.

($\Leftarrow$) Suppose $e_p \leqslant f_p$, define $d_p \coloneqq f_p - e_p \geqslant 0$ for every prime $p$. Let $c \coloneqq 2^{d_2} 3^{d_3} \cdots p^{d_p} \cdots$, then necessarily $b = ac$, and therefore $a \mid b$. □

## 2.2. GCD & LCM via Factorisation

**Lemma 2.7.** *With the notation as in Proposition 2.6, we have*

$$\gcd(a, b) = 2^{\min(e_2, f_2)} 3^{\min(e_3, f_3)} \cdots p^{\min(e_p, f_p)} \cdots$$

$$\operatorname{lcm}(a, b) = 2^{\max(e_2, f_2)} 3^{\max(e_3, f_3)} \cdots p^{\max(e_p, f_p)} \cdots$$

*In particular, $ab = \gcd(a, b) \operatorname{lcm}(a, b)$.*

*Proof.* Before we prove the result, let us remark how it gives us $ab = \gcd(a, b) \operatorname{lcm}(a, b)$.

Assume that gcd and lcm have the given prime factorisation. Since $e_p + f_p = \min(e_p, f_p) + \max(e_p, f_p)$, we necessarily obtain $ab = \gcd(a, b) \operatorname{lcm}(a, b)$ by comparing prime factorisations of both products.

Now, write $g \coloneqq \gcd(a,b) = 2^{h_2}3^{h_3}\cdots p^{h_p}$. Since $g \mid a$ and $g \mid b$, therefore $h_p \leqslant e_p$ and $h_p \leqslant f_p$, using Proposition 2.6. Hence $h_p \leqslant \min(e_p, f_p)$.

Let $d = 2^{\min(e_2,f_2)}3^{\min(e_3,f_3)}\cdots p^{\min(e_p,f_p)}\cdots$, since $\min(e_p,f_p) \leqslant e_p$ and $\min(e_p,f_p) \leqslant f_p$, therefore $d \mid a$ and $d \mid b$, using Proposition 2.6. Hence $d \mid g$, by definition of gcd, and necessarily $\min(e_p,f_p) \leqslant h_p$, using Proposition 2.6.

Therefore $h_p = \min(e_p, f_p)$, and hence $\gcd(a,b) = 2^{\min(e_2,f_2)}3^{\min(e_3,f_3)}\cdots p^{\min(e_p,f_p)}\cdots$.

A similar argument gives us the result for lcm. □

**Example 2.8.** Consider

$$a = 180 = 2^2\cdot 3^2\cdot 5 = 2^2\cdot 3^2\cdot 5^1\cdot 7^0$$

$$b = 126 = 2\cdot 3^2\cdot 7 = 2^1\cdot 3^2\cdot 5^0\cdot 7^1$$

Find their gcd and lcm. How many positive divisors of $b$ can there be?

*Answer.* By Lemma 2.7, we have

$$\gcd(a,b) = 2^1\cdot 3^2\cdot 5^0\cdot 7^0 = 18$$

$$\operatorname{lcm}(a,b) = 2^2\cdot 3^2\cdot 5^1\cdot 7^1 = 1260$$

Now, any positive divisor of $b$ is necessarily of the form $d = 2^{e_2}\cdot 3^{e_3}\cdot 7^{e_7}$. By Proposition 2.6,

$$0 \leqslant e_2 \leqslant 1, \quad 0 \leqslant e_3 \leqslant 2, \quad 0 \leqslant e_7 \leqslant 1,$$

Since $e_2$ has two choices, $e_3$ has three and $e_7$ has two as well, the number of positive divisor of $b$ is $2\cdot 3\cdot 2 = 12$. 👌

**Example 2.9** (in-class)**.** Consider

$$a = 3^2\cdot 5^4\cdot 11^1\cdot 17^3$$

$$b = 2^3\cdot 3^2\cdot 5^3\cdot 7^2$$

Compute the prime factorisation of their gcd and lcm. How many positive divisors does $a$ have?

## 2.3. Towards Arithmetic Functions

**Remark 2.10.** Given an integer $n$, we may write its prime factorisation in two equivalent ways. Recall that up until now, we have written the prime factorisation of $n$ as

$$n = 2^{e_2}3^{3_e}\cdots p^{e_p}\cdots$$

where $e_p \geqslant 0$ for any prime $p$ and $e_p = 0$ for every prime $p > n$.

Let $p_1, p_2, \ldots, p_r$ be the finitely many primes for which $e_{p_i} > 0$, then letting $\varepsilon_i \coloneqq e_{p_i}$ for $1 \leqslant i \leqslant r$, we may write

$$n = p_1^{\varepsilon_1}p_2^{\varepsilon_2}\cdots p_r^{\varepsilon_r}$$

An important consequence of prime factorisation is the following theorem.

**Theorem 2.11.** *Let $a$ and $b$ be coprime positive integers*

(i) *If $u$ and $v$ are positive divisors of $a$ and $b$ respectively, then $uv \mid ab$.*

(ii) *Conversely, for any positive divisor $w$ of $ab$, there exist unique positive integers $u$ and $v$ such that $u \mid a$ and $v \mid b$, and $w = uv$.*

*Put another way, there is a well-defined bijective function*

$$\Phi\colon \mathscr{D}(a)\times\mathscr{D}(b) \to \mathscr{D}(ab), \quad \Phi(u,v) = uv$$

*where $\mathscr{D}(n) \coloneqq \{d \in \mathbb{Z}_+ \,:\, d \mid n\}$ is the set of positive divisors of an integer $n$.*

*Proof.* (i) follows from Problem 1.2. Let us prove (ii).

Consider a positive divisor $w$ of $ab$, where the prime factorisations of $a$ and $b$ are written as

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, \quad b = q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s}$$

Since $\gcd(a, b) = 1$, necessarily $p_i \neq q_j$ for all $1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant s$. Therefore

$$ab = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s},$$

and hence

$$w = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r} q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s},$$

where $0 \leqslant h_i \leqslant e_i$ and $0 \leqslant k_j \leqslant f_j$, by Proposition 2.6. Letting $u = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}$ and $v = q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s}$, gives us $w = uv$ and, again by Proposition 2.6, $u \mid a$ and $v \mid b$.

This proves surjectivity of $\Phi$, injectivity follows from uniqueness of prime factorisation. □

**Notation.** For a finite set $S$, we denote by $\#S$ its cardinality, i.e., the number of elements in $S$.

**Definition 2.12.** For any positive integer $n$, define the **0th divisor-sum function** as

$$\sigma_0(n) \coloneqq \#\mathscr{D}(n) = \sum_{d \in \mathscr{D}(n)} d^0,$$

i.e., $\sigma_0(n)$ equals the number of positive divisors of $n$. Therefore it is also called the **number-of-divisors function**.

For example, $\sigma_0(6) = \#\{1, 2, 3, 6\} = 4$

**Remark 2.13.** $\sigma_0(n) = 1$ if and only if $n = 1$.

If $n > 1$, then $\sigma_0(n) \geqslant 2$ since $n$ always has 1 and $n$ as divisors. In fact, $\sigma_0(n) = 2$ if and only if $n$ is prime.

**Corollary 2.14.** *For positive integers $a, b$ such that $\gcd(a, b) = 1$, we have $\sigma_0(ab) = \sigma_0(a)\sigma_0(b)$.*

*Proof.* Recall that the sets $\mathscr{D}(a) \times \mathscr{D}(b)$ and $\mathscr{D}(ab)$ are bijective via the map $\Phi$, as seen in Theorem 2.11. Therefore

$$\sigma_0(a)\sigma_0(b) = \#\mathscr{D}(a) \cdot \#\mathscr{D}(b) = \#\left(\mathscr{D}(a) \times \mathscr{D}(b)\right) = \#\mathscr{D}(ab) = \sigma_0(ab)$$

as claimed. □

**Corollary 2.15.** *For a positive integer $n$ with prime factorisation $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, we have*

$$\sigma_0(n) = (e_1 + 1)(e_2 + 1) \cdots (e_r + 1)$$

*Proof.* Let $p$ be a prime, and consider $p^e$ for any integer $e \geqslant 0$. Then note that $\mathscr{D}(p^e) = \left\{p^f \ : \ 0 \leqslant f \leqslant e\right\}$. Therefore

$$\sigma_0(p^e) = e + 1.$$

Now, consider $n$ as in the statement, then

$$\begin{aligned}
\sigma_0(n) &= \sigma_0(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) \\
&= \sigma_0(p_1^{e_1})\, \sigma_0(p_2^{e_2}) \cdots \sigma_0(p_r^{e_r}) && \text{using Corollary 2.14 iteratively} \\
&= (e_1 + 1)(e_2 + 1) \cdots (e_r + 1) && \text{using } \sigma_0(p^e) = e + 1 \text{ for primes } p, \text{ as shown above}
\end{aligned}$$

Thus, we have proven our claim. □

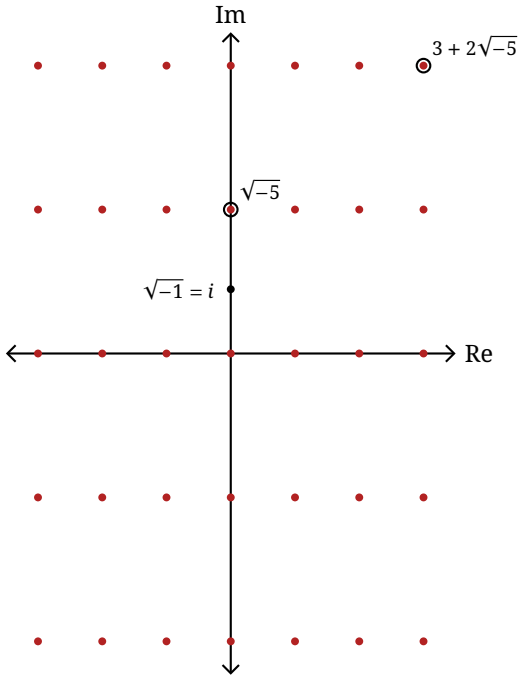
## 2.4. Appreciating Uniqueness of Prime Factorisation

First, we make a small extension to our definitions: any non-zero integer can be uniquely written as

$$n = \pm 2^{e_2} \cdot 3^{e_3} \cdots p^{e_p} \cdots, \quad \text{such that } e_p \geqslant 0 \text{ and } e_p = 0 \text{ for all } p > |n|$$

$\pm 1$ are called units.

**Definition 2.16.** Define $\mathcal{O} = \mathbb{Z}[\sqrt{-5}] \coloneqq \left\{a + b\sqrt{-5} \ : \ a, b \in \mathbb{Z}\right\} \subseteq \mathbb{C}$, shown as a (rectangular) grid of points in $\mathbb{C}$ below




We read $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$ as "$\mathbb{Z}$ *adjoined* $\sqrt{-5}$".

**Fact.** $\mathcal{O}$ is "closed" under addition, subtraction and multiplication, i.e., adding, subtracting or multiplying any two elements of $\mathcal{O}$ produces another element that continues to lie in $\mathcal{O}$. Moreover, $\mathcal{O}$ also contains 0 and 1.

In particular, $\mathcal{O}$ is a (commutative) ring.

*Sketch of Fact.* Let $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$ be elements of $\mathcal{O}$, so $a, b, c, d \in \mathbb{Z}$. Then

$$\alpha + \beta = (a + c) + (b + d)\sqrt{-5} \in \mathcal{O}$$

$$-\beta = (-c) + (-d)\sqrt{-5} \in \mathcal{O}$$

$$\alpha\beta = (ac - 5bd) + (ad + bc)\sqrt{-5} \in \mathcal{O}$$

Since $a + c$, $b + d$, $-c$, $-d$, $(ac - 5bd)$ and $(ad + bc)$ are all integers as well.

Finally, $0 = 0 + 0\sqrt{-5} \in \mathcal{O}$ and $1 = 1 + 0\sqrt{-5} \in \mathcal{O}$. □

We will mimic the definition of prime numbers in $\mathbb{Z}$ to introduce an analogous notion in $\mathcal{O}$.

**Definition 2.17.** A non-zero element $\alpha \in \mathcal{O}$ is called **irreducible** if

(I1) $\alpha \neq \pm 1$

(I2) for any $\beta, \gamma \in \mathcal{O}$ such that $\alpha = \beta\gamma$, then necessarily $\beta = \pm 1$ or $\gamma = \pm 1$

**Definition 2.18.** We say two elements $\alpha, \beta \in \mathcal{O}$ are **associates** if $\alpha = \pm\beta$.

**Remark 2.19.** Elements in $\mathcal{O}$, much like $\mathbb{Z}$, can be written as a product of irreducible elements, i.e., they have a factorisation into irreducibles.

But this factorisation *need not be unique*, i.e., $\mathcal{O}$ does not admit a notion of *unique* factorisation into irreducibles.

We illustrate this fact with an example, the content of which is Problem 2.8. Note

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

There exist no $\gamma \in \mathcal{O}$ such that $2\gamma = 1 + \sqrt{-5}$. More generally, $2,\ 3$ and $1 \pm \sqrt{-5}$ are all non-associate irreducibles.

## 2.5. Remarks on Distribution of Primes

**Distribution of prime numbers I. *Larger scale***

**Theorem 2.20** (Infinitude of Primes; Euclid)**.** *There are infinitely many primes.*

*Proof.* Towards a contradiction, assume there are finitely many primes

$$p_1 = 2,\ p_2 = 3, \ldots,\ p_N$$

Consider $M = p_1 p_2 \cdots p_N + 1$, since every positive integer has a prime factor, $p_i \mid M$ for some $1 \leqslant i \leqslant N$.

But also observe that $p_i \mid p_1 p_2 \cdots p_N$, and therefore $p_i$ divides $M - p_1 p_2 \cdots p_N = 1$, giving us a contradiction.

Hence, there are infinitely many primes. □

More quantitatively,

**Definition 2.21.** For any real number $x > 0$,

$$\pi(x) \coloneqq \#\{p \in \mathbb{Z} \ :\ p \text{ is a prime}, p \leqslant x\} = (\text{number of primes} \leqslant x)$$

$\pi$ is called the **prime counting function**. For example, $\pi(1.5) = 0, \pi(23) = \#\{2, 3, 5, 7, 11, 13, 17, 19, 23\} = 9$.

**Remark 2.22.** So, Euclid's theorem on infinitude of primes says that as $\pi(x) \to \infty$ as $x \to \infty$.

Computing $\pi(x)$ is hard, one can do it for $x \sim 10^{13}$ but not for, say, $x \sim 10^{10^{10}}$.

**Question.** *Do we have an asymptotic formula for $\pi(x)$? That is, can we find a simpler function $f$ such that*

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

*If so, can we bound the "error" $|\pi(x) - f(x)|$ in terms of $x$?*

**Theorem 2.23** (Prime Number Theorem; Hadamard, de la Vallée Poussin, 1896)**.**

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

*That is, for high enough values of $x$, we can estimate $\pi(x)$ by the function $\dfrac{x}{\log(x)}$.*

**Conjecture A** (a consequence of the Riemann Hypothesis)**.** *For all $x \geqslant 2657$,*

$$|\pi(x) - \mathrm{li}(x)| < \frac{1}{8\pi}\sqrt{x}\log x,$$

*where* $\mathrm{li}(x) = \displaystyle\int_0^x \frac{dt}{\log t} \sim \frac{x}{\log(x)}$ *is the* **logarithmic integral**.

**Distribution of prime numbers II.** ***Smaller scale***

$$\underbrace{2,\ 3}_{1},\ 5,\ 7,\ 11, 13,\ \ldots,\ 263,\ 269,\ 271,\ 277,\ \ldots,$$
$$877,\ 881,\ 883,\ 887,\ 907,\ 911,\ 919,\ \ldots$$

Since all primes larger than 2 are odd, the gap between them is always even; except between 2 and 3.

**Definition 2.24.** **Twin primes** are a pair of primes $(p, q)$ such that $|p - q| = 2$.

**Conjecture B.** *There are infinitely many twin primes.*

**Theorem 2.25.** *There are infinitely many pairs $(p, q)$ of primes such that*

$$(\sim 2013, \text{Y. Zhang}) \quad |q - p| < 7 \cdot 10^7$$
$$(\sim 2014, \text{Polymath8}) \quad |q - p| < 246$$

## Problems

**Problem 2.1.** Let $a, b$ and $n$ be positive integers, and $a^n \mid b^n$, prove that $a \mid b$.

**Problem 2.2.** Recall the *factorial* of a number: $n! = 1 \cdot 2 \cdots (n-1) \cdot n$.

Prove that if $n \geqslant 1$, then no number in the following list of $n - 1$ numbers

$$n! + 2,\ n! + 3,\ \ldots,\ n! + n$$

is a prime.

This problem illustrates that we can produce a list of $n$ consecutive numbers, called a **prime desert of length $n$**, for any positive integer $n$. Therefore there is *no general bound on the length of gaps between all primes*.

**Problem 2.3.** Let $a, b > 0$ be integers. Prove that

$$\gcd(a^k, b^k) = \gcd(a, b)^k \quad \text{and} \quad \operatorname{lcm}(a^k, b^k) = \operatorname{lcm}(a, b)^k$$

for any integer $k \geqslant 0$. This generalises Problem 1.8.

**Problem 2.4.** This problem is concerned with the prime factorisation of factorials.

(a) Find the prime decomposition of 13! and 20!, and compute $\sigma_0(13!)$ and $\sigma_0(20!)$.

(b) How many zeros would you find at the end of 100!, if you expanded it out in base ten?

(c) Let $e_p$ be the exponent of a prime $p$ in the prime decomposition of $n!$. Prove that

$$e_p = \sum_{i \geqslant 0} \left\lfloor \frac{n}{p^i} \right\rfloor$$

Use this to show that $e_p \leqslant \dfrac{n}{p-1}$.

**Problem 2.5.** We call an integer $n$ a **perfect square** if $n = k^2$ for some integer $k$.

(a) Prove that $n$ is a perfect square if and only if the exponents in its prime factorisation are even.

(b) Prove that $n$ is a perfect square if and only if its has odd-many positive divisors.

(c) **(challenge)** Let $n$ be a perfect square, characterise the divisor $k$ such that $n = k^2$.

**Problem 2.6.** Prove that if $n$ is a positive integer, and $\sigma_0(n)$ is prime then $n$ is a power of a prime number.

**Problem 2.7** (Mersenne, 1644)**.** What is the smallest positive integer with precisely 60 positive divisors?

**Problem 2.8.** Recall from Definition 2.16 the following subset of $\mathbb{C}$

$$\mathcal{O} = \{a + b\sqrt{-5} \ : \ a, b \in \mathbb{Z}\}.$$

(a) Consider the function $\mathrm{N}\colon \mathcal{O} \to \mathbb{Z}$, called the **norm function**, defined as

$$\mathrm{N}(a + bi\sqrt{5}) = a^2 + 5b^2.$$

Prove that, for any $\alpha, \beta \in \mathcal{O}$, one has

$$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)N(\beta)$$

(b) Recall the notation of irreducible elements from Definition 2.17. Prove that the following 4 elements

$$2,\ 3,\ 1 + \sqrt{-5} \text{ and } 1 - \sqrt{-5}$$

are irreducible.

(c) Show that there exists no element $\gamma \in \mathcal{O}$ such that $2\gamma = 1 + \sqrt{-5}$ or $2\gamma = 1 - \sqrt{-5}$.

Conclusion: Factorisation into irreducibles in $\mathcal{O}$ is not unique: $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

**Problem 2.9.** Let $T = \{1, 4, 7, 10, 13, 16, 19, \ldots\} = \{3k + 1 \ : \ k \in \mathbb{N}\}$.

An element of $T$ is called **irreducible** if it is not 1 and its only factors *within $T$* are 1 and itself.

(a) Suppose $a, b \in T$ and $c$ is a positive integer. Prove that if $a = bc$, then $c \in T$.

(b) Demonstrate that every element of $T$ can be factored as a product of irreducible elements of $T$.

(c) Find three examples of elements of $T$ with *non-unique* factorisation into irreducibles.

**Problem 2.10.** Let $H = \{1, 5, 9, 13, 17, \ldots\} = \{4k + 1 \ : \ k \in \mathbb{N}\}$, this is called the **Hilbert monoid**.

As in Problem 2.9, we can define an *irreducible element* of $H$.

We call an element $h \in H$ a **prime element** if $h \mid ab$, for some $a, b \in H$, then either $h \in a$ or $h \in b$.
(this definition mimics the property of prime numbers we saw in Corollary 2.4)

Find an example of an $h \in H$ which is irreducible and not prime, and prove it so.

**Problem 2.11.** For this problem, you may want to review single variable Calculus.

Recall the logarithmic integral from Conjecture A

$$\mathrm{li}(x) = \int_0^x \frac{dt}{\log(t)}$$

(a) What is $\dfrac{d}{dx}\mathrm{li}(x)$?

(b) Prove that $\mathrm{li}(x) \sim \dfrac{x}{\log(x)}$, i.e., show the following

$$\lim_{x\to\infty} \frac{x/\log(x)}{\mathrm{li}(x)} = 1$$

# 3. Arithmetic Functions I

**Definition 3.1.** An **arithmetic function** is a function $f\colon \mathbb{Z}_+ \to \mathbb{C}$.

That is, it is a complex-valued function whose domain is the set of positive integers.

## 3.1. Divisor-sum Functions

**Definition 3.2.** An arithmetic function $f$ is called **multiplicative** if, for coprime positive integer $a, b$, we have

$$f(ab) = f(a)f(b)$$

**Example 3.3.**

(1) Fix $k \in \mathbb{R}$ and define $f_k(n) = n^k$. Then,

$$f_k(ab) = (ab)^k = a^k b^k = f_k(a)f_k(b)$$

(2) Recall the number-of-divisors function $\sigma_0 : \mathbb{Z}_+ \to \mathbb{C}$, where

$$\sigma_0(n) = (\text{number of positive divisors of } n) = \sum_{d\in\mathscr{D}(n)} d^0.$$

Note that Corollary 2.14 tells us that $\sigma_0$ is multiplicative.

The coprime assumption is essential. For example, consider $a = 2$ and $b = 4$, then $\sigma_0(2 \cdot 4) = \sigma_0(8) = 4$.

But $\sigma_0(2) = 2$ and $\sigma_0(4) = 3$, therefore giving us $\sigma_0(2)\sigma_0(4) = 6 \neq 4 = \sigma_0(2 \cdot 4)$.

(3) **(non-example)** Consider the function $f : \mathbb{Z}_+ \to \mathbb{C}$ given as $f(n) = 2n + 1$. For $a = 2$ and $b = 3$, we have

$$f(2) = 3, \qquad f(3) = 5, \qquad f(2 \cdot 3) = f(6) = 11$$

Of course, $f(2 \cdot 3) = 11 \neq 15 = f(2)f(3)$.

We generalise the function $\sigma_0$.

**Definition 3.4.** Let $k \in \mathbb{R}$, define the **$k^{\text{th}}$ divisor-sum function** as

$$\sigma_k : \mathbb{Z}_+ \to \mathbb{C}, \quad \sigma_k(n) = \sum_{d\in\mathscr{D}(n)} d^k$$

For example, consider $k = 2$ and $\sigma_2(6) = 1^2 + 2^2 + 3^2 + 6^2 = 50$.

The case when $k = 1$, we get $\sigma_1(n) = \sum_{d\in\mathscr{D}(n)} d$, which is also called the **sum-of-divisors function**.

**Theorem 3.5.** *For any $k \in \mathbb{R}$, $\sigma_k$ is multiplicative.*

*Proof.* Let $a, b$ be positive integers such that $\gcd(a, b) = 1$, then

$$\begin{aligned}
\sigma_k(ab) = \sum_{w\in\mathscr{D}(ab)} w^k &= \sum_{(u,v)\in\mathscr{D}(a)\times\mathscr{D}(b)} (uv)^k && \text{by Theorem 2.11} \\
&= \sum_{u\in\mathscr{D}(a)} \sum_{v\in\mathscr{D}(b)} u^k v^k \\
&= \sum_{u\in\mathscr{D}(a)} \left( u^k \cdot \sum_{v\in\mathscr{D}(b)} v^k \right) = \sum_{u\in\mathscr{D}(a)} u^k \cdot \sigma_k(b) = \sigma_k(b) \left( \sum_{u\in\mathscr{D}(a)} u^k \right) = \sigma_k(b)\sigma_k(a)
\end{aligned}$$

as claimed. □

We're now ready to introduce a strategy to compute $\sigma_k(n)$ for any given $k$ and $n$.

**Proposition 3.6.** *Let $x \neq 1$ be a real number and $e \geqslant 0$ be an integer. Then*

$$1 + x + x^2 + \cdots + x^e = \frac{x^{e+1} - 1}{x - 1}$$

*Proof.* Let $S = 1 + x + x^2 + \cdots + x^{e-1} + x^e$, then

$$\begin{aligned} xS &= x + x^2 + \cdots + x^e + x^{e+1} \\ &= x + x^2 + \cdots + x^e + x^{e+1} + 1 - 1 \\ &= (1 + x + x^2 + \cdots + x^e) + x^{e+1} - 1 \\ &= S + x^{e+1} - 1 \end{aligned}$$

Therefore $(x-1)S = xS - S = x^{e+1} - 1$. Since $x \neq 1$, hence $S = \dfrac{x^{e+1} - 1}{x - 1}$. □

**Corollary 3.7.** *If $p$ is a prime, $e \geqslant 0$ an integer and $k \neq 0$, then*

$$\sigma_k(p^e) = \frac{(p^{e+1})^k - 1}{p^k - 1}$$

*Proof.* Note that for any $\mathscr{D}(p^e) = \left\{p^h \ : \ 0 \leqslant h \leqslant e\right\}$. Therefore

$$\begin{aligned} \sigma_k(p^e) &= (p^0)^k + (p^1)^k + (p^2)^k + \cdots + (p^{e-1})^k + (p^e)^k \\ &= 1 + p^k + (p^k)^2 + \cdots + (p^k)^e \\ &= \frac{(p^k)^{e+1} - 1}{p^k - 1} \qquad \text{taking } x = p^e \text{ in Proposition 3.6} \end{aligned}$$

since $k \neq 0$ and so $p^k \neq 1$. □

**Example 3.8.** Compute $\sigma_3(12)$.

*Answer.* First note that $12 = 2^2 \cdot 3$. Since $\gcd(2^2, 3) = 1$, therefore

$$\begin{aligned} \sigma_3(12) &= \sigma_3(2^2)\sigma_3(3) \\ &= \frac{(2^{2+1})^3 - 1}{2^3 - 1} \cdot \frac{(3^{1+1})^3 - 1}{3^3 - 1} \\ &= 73 \cdot 28. \end{aligned}$$

Hence $\sigma_3(12) = 2044$. □

**Remark 3.9.** Our general strategy to compute $\sigma_k(n)$, when $k > 0$, is as follows:

1. Consider the prime factorisation of $n$, say $n = p_1^{e_1} \cdots p_r^{e_r}$
2. Since $\gcd(p_i, p_j) = 1$, therefore $\gcd(p_i^{e_i}, p_j^{e_j}) = 1$ for $i \neq j$; see Problem 1.3 (vii).
3. Hence $\sigma_k(n) = \sigma_k(p_1^{e_1}) \cdots \sigma_k(p_r^{e_r})$.
4. Apply Corollary 3.7 to $\sigma_k(p_i^{e_i})$.

**Example 3.10** (in-class)**.**

(i) Express $\sigma_4(27)$ as $\dfrac{3^a-1}{3^b-1}$ for some positive integers $a, b$.

(ii) Suppose we're given a multiplicative function $f$, and we've been told

$$f(2)=4, \quad f(3)=11, \quad f(4)=3, \quad f(6)=33, \quad f(8)=5$$

Do we know enough to compute $f(24)$? If yes, compute it. If not, why not?

## 3.2. Perfect Numbers & Mersenne Primes

**Definition 3.11.** Let $n$ be a positive integer. We call a positive divisor $d$ of $n$ a **proper divisor** if $d < n$.

- Say $n$ is **perfect** if the sum of its proper divisors equals $n$. Or, equivalently, if $\sigma_1(n) = 2n$.
- Say $n$ is **deficient** if $\sigma_1(n) < 2n$.
- Say $n$ is **abundant** if $\sigma_1(n) > 2n$.

**Example 3.12.**

(1) Let $n = p$ be a prime, then $\sigma_1(p) = 1 + p < 2p$. Therefore primes are deficient.

(2) Let $n = 6$, then $\sigma_1(6) = 1 + 2 + 3 + 6 = 6 + 6$. Therefore 6 is perfect.

(3) Let $n = 12$, then $\sigma_1(12) = 1 + 2 + 3 + 4 + 6 + 12 > 24$. Therefore 12 is abundant.

**Remark 3.13.** There are about fifty known perfect numbers: 6, 28, 496, 8128, 33550336, ... (about fifty).

To see the entire list, see sequence A000668 in the On-Line Encyclopedia of Integer Sequences (OEIS).

All known perfect numbers are *even*.

**Open Question C.** *There remain important unanswered question about perfect numbers.*

- *Are there infinitely many perfect numbers?*
- *Are there any* odd *perfect numbers?*

There is a systematic way to generate even perfect numbers and this is related to the following question.

**Question.** *For which $n \in \mathbb{Z}_+$, is $2^n - 1$ prime?*

**Proposition 3.14.** *If a positive integer $n$ is such that $2^n - 1$ is prime, then $n$ is prime.*

*Proof.* Suppose, for sake of contradiction, $n$ is not prime. Then $n = ab$, for some $1 < a, b < n$, which gives us

$$\begin{aligned} 2^n - 1 &= 2^{ab} - 1 \\ &= (2^a)^b - 1^b \\ &= (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1) \qquad \text{using Problem 3.1 (⊛)} \end{aligned}$$

Since $1 < a, b < n$, neither $2^a - 1$ nor $(2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1$ equal 1.

Therefore $2^n - 1 = 2^{ab} - 1$ is composite, giving us a contradiction. Hence $n$ is prime. □

**Remark 3.15.** The converse of Proposition 3.14 is *not true*, that is, if $n$ is prime then $2^n - 1$ is not necessarily prime.

For example, one has $2^{11} - 1 = 2047 = 23 \cdot 89$.

**Definition 3.16.** A **Mersenne prime** is a prime number of the form $2^p - 1$ for some prime $p$.

Denote the Mersenne prime with respect to $p$ as $M_p = 2^p - 1$

For example, $M_3 = 2^3 - 1 = 7$ is a Mersenne prime, but 11 is not since $11 + 1$ is not a power of 2.

**Theorem 3.17** (Euclid)**.** *Let $M_p$ be a Mersenne prime, then $N_p = 2^{p-1}M_p = 2^{p-1}(2^p - 1)$ is an even perfect number.*

The Mersenne prime $M_2 = 3$ corresponds to the even perfect number $N_2 = 6$; while $M_3 = 7$ corresponds to $N_3 = 28$ and $M_5 = 31$ corresponds to $N_5 = 496$.

*Proof.* We wish to show that $\sigma_1(N_p) = 2N_p$. Since $M_p$ is an odd prime, necessarily $\gcd(2^{p-1}, M_p) = 1$. Observe

$$\begin{aligned}
\sigma_1(N_p) &= \sigma_1(2^{p-1}M_p) \\
&= \sigma_1(2^{p-1}) \cdot \sigma_1(M_p) && \text{since } \gcd(2^{p-1}, M_p) = 1 \text{ and multiplicativity of } \sigma_1 \\
&= \frac{2^{p-1+1} - 1}{2 - 1} \cdot (1 + M_p) && \text{by Corollary 3.7 and since } M_p \text{ is prime} \\
&= 2^p(2^p - 1) \\
&= 2 \cdot 2^{p-1}M_p \\
&= 2N_p
\end{aligned}$$

Therefore $N_p$ is an even perfect number. □

**Remark 3.18.** Theorem 3.17 is the final theorem on Number Theory in Euclid's *Elements* (circa 300 BCE). About a millennium later (circa 1000 CE), it was conjectured by Ibn al-Haytham, a mathematician and physicist during the Islamic Golden Age (also called the "father of modern optics"), that the converse also holds true. But he was unable to provide a proof and it would not be proved until much later by Euler, about 2000 years after Euclid's theorem above.

**Theorem 3.19** (Euler, 1849)**.** *Suppose $N$ is an even perfect number, then there exists a prime number $p$ such that $N = N_p$, as in Theorem 3.17.*

*Proof.* Let $N$ have the following prime factorisation

$$N = 2^{e_2}3^{e_3} \cdots p^{e_p} \cdots,$$

where $e_p \geqslant 0$ (and $e_p = 0$ for all $p > N$). Define $p := e_2 + 1$ and $q := N/2^{e_2} = 3^{e_3} \cdots p^{e_p} \cdots$. In particular, $N = 2^{p-1}q$. Note that $\gcd(2^{p-1}, q) = 1$ since $2 \nmid q$. Since $N$ is perfect, we have

$$\begin{aligned}
2^p q = 2N = \sigma_1(N) &= \sigma_1(2^{p-1}q) \\
&= \sigma_1(2^{p-1}) \cdot \sigma_1(q) && \text{since } \sigma_1 \text{ is multiplicative} \\
&= (2^p - 1) \cdot \sigma_1(q)
\end{aligned}$$

Therefore,

$$\sigma_1(q) = q \cdot \left(\frac{2^p}{2^p - 1}\right) = q \cdot \left(\frac{1}{2^p - 1} + 1\right) = \frac{q}{2^p - 1} + q$$

Since $\sigma_1(q)$ and $q$ are integers, so is $\sigma_1(q) - q = \dfrac{q}{2^p - 1}$. That is,

$$d := \frac{q}{2^p - 1} \in \mathbb{Z}_+$$

Hence, $q = d \cdot (2^p - 1)$ and thus $d \mid q$.

Since $N$ is even, $p-1=e_2\geqslant 1$, so $2^p-1>1$ and therefore $d\neq q$, i.e., $d$ is a proper divisor of $q$.

In summary, $d$ is a proper divisor of $q$ and $\sigma_1(q)=q+d$. We will now argue by contradiction that $q$ is prime.

CASE I: $q=1$. Then $d=\sigma_1(1)-1=0$, giving us a contradiction since $d$ is positive.

CASE II: $q$ is composite. Then $q=ab$, for some positive integers $a,b$ such that $1<a,b<n$.

We have the following two possibilities

- *a or b equal d.* Suppose $a=d$, without loss of generality, then
$$d=\sigma_1(q)-q\geqslant d+b>d.$$
We have arrived at a contradiction.
- *neither a nor b equal d.* Then
$$d=\sigma_1(q)-q\geqslant d+a+b>d.$$
We have yet again arrived at a contradiction.

Thus $q$ is prime, and since $d$ is a proper divisor, we conclude $d=1$. Therefore $q=2^p-1$ is a prime, and hence so is $p$ by Proposition 3.14.

Thus, $q=M_p$ is a Mersenne prime and $N=2^{p-1}M_p=N_p$. □

**Remark 3.20.** Theorems 3.17 and 3.19 are collectively called the *Euclid-Euler theorem* and establish a one-to-one correspondence between even perfect numbers and Mersenne primes.

The currently known perfect numbers all come from the known list of Mersenne primes.

Largest known prime numbers have usually been Mersenne primes. The currently largest known prime number is $2^{136279841}-1$; it was found on October 12, 2024 by Luke Durant and volunteered to the **Great Internet Mersenne Prime Search (GIMPS)**. The largest known even perfect number corresponds to this Mersenne Prime and is 1701411834604692317316873037158841057 27.

## PROBLEMS

**Problem 3.1.** In this problem, we will extend Proposition 3.6.

(a) Verify that the following identity holds for any $x$
$$x^{e+1}-1=(x-1)(x^e+x^{e-1}+\cdots+x+1)$$

(b) Let $x,\ y$ be real numbers such that $y\neq 0$. Use (a) to prove that
$$x^{e+1}-y^{e+1}=(x-y)(x^e+x^{e-1}y+\cdots+xy^{e-1}+y^e)$$

(c) Verify that the identity in (b) holds even when $y=0$.

In conclusion, you have proven the identity: for any real number $x$ and $y$ and integer $e\geqslant 0$
$$x^{e+1}-y^{e+1}=(x-y)(x^e+x^{e-1}y+\cdots+xy^{e-1}+y^e) \qquad (\circledast)$$

**Problem 3.2.** Compute $\sigma_1(N)$ for the three numbers $N=28$, $N=111$, and $N=240$. Classify $N$ as abundant, deficient or perfect.

**Problem 3.3** (Mersenne, 1644)**.** Describe all circumstances under which $\sigma_1(n)$ is odd.

**Problem 3.4.** Find a short formula for $\sigma_0(p)+\sigma_1(p)+\cdots+\sigma_k(p)$ whenever $p$ is a prime number.

**Problem 3.5.** Prove that for every positive integer $n$, we have

$$\sigma_k(n) = \sigma_{-k}(n)n^k.$$

Conclude that $n$ is perfect if and only if $\sigma_{-1}(n) = 2$.

**Problem 3.6.** Prove that if $n$ is a perfect square, then $n$ is not a perfect number.

**Problem 3.7.** Let $a$ and $b$ be positive integers. We say $a$ and $b$ are **amicable numbers** if $\sigma_1(a) = \sigma_1(b) = a + b$.

In particular, $a$ is a perfect number if it is amicable with itself.

Prove the following result of *Thabit ibn Kurrah* (836-901): if $p = 3 \cdot 2n - 1 - 1$ is prime and $q = 3 \cdot 2^n - 1$ is prime, and $r = 9 \cdot 2^{2n-1} - 1$ is prime, then $a = 2^n \cdot p \cdot q$ and $b = 2^n \cdot r$ are amicable numbers.

Find a pair of amicable numbers by finding such prime numbers $p$, $q$, and $r$.

**Problem 3.8.** We say that a positive integer $n$ is **square-free** if $n$ is not divisible by $p^2$ for any prime number $p$. Necessarily, the prime factorisation of such an $n$ is of the form

$$n = p_1 p_2 \cdots p_t$$

For example, 15 and 37 are square-free, but $24 = 2^2 \cdot 6$ and $49 = 7^2$ are not.

Consider the following arithmetic function, the **Möbius function** (named after A.F. Möbius, popularly known for his strip),

$$\mu\colon \mathbb{Z}_+ \to \mathbb{C}, \quad \mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \text{ is not square-free} \\ (-1)^t & \text{if } n \text{ is square-free and has exactly } t \text{ prime divisors.} \end{cases}$$

(a) Compute $\mu(n)$ for $n = 1, \ldots, 15$.

(b) Prove that $\mu$ is multiplicative, i.e., we have $\mu(ab) = \mu(a)\mu(b)$ whenever $a$ and $b$ are positive coprime integers.
Hint: proceed by cases, taking cue from the definition of $\mu$.

(c) Let $n > 1$ be an integer. Prove that

$$\sum_{d \in \mathscr{D}(n)} \mu(d) = 0.$$

In other words, the sum of $\mu(d)$, as $d$ ranges over all the positive divisors of $n$, is equal to 0.

Hint: the binomial expansion will be useful $(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$, where the binomial coefficient $\binom{n}{i}$ counts the number of ways to choose $i$ things from a set of $n$-many things.

**Problem 3.9.** Let $f$ and $g$ be two arithmetic functions. Define a new arithmetic function $h\colon \mathbb{Z}_+ \to \mathbb{C}$ by the formula:

$$h(n) = \sum_{d \in \mathscr{D}(n)} f(d) g\left(\frac{n}{d}\right).$$

(a) Let $f(n) = n$ and $g(n) = \mu(n)$, as defined in Problem 3.8. Compute the values of $h(n)$ for $n = 1, \ldots, 12$.

(b) Prove that if $f$ and $g$ are multiplicative, then $h$ is a multiplicative function as well.
Hint: the method of proof we used in Theorem 3.5 will be helpful.

The new function $h$ is called the **divisor** (or **Dirichlet**) **convolution** of $f$ and $g$, and is denoted by $f * g$. The idea originates from Fourier analysis. We will explore this notion more later in the course (see Section 8).

# 4. Rational Numbers

## 4.1. Fractions & Irrationality

**Definition 4.1.** A **rational number** is a number of the form $a/b$, where $a, b$ are integers and $b \neq 0$.

A **fraction** is an expression of the form $a/b$, where $a, b$ are integers and $b \neq 0$.

For example, $\frac{2}{3}$ and $\frac{4}{6}$ are distinct fractions but equal as rational numbers.

**Definition 4.2.** Say a fraction $a/b$ is in **standard form** if $b > 0$, and it is **reduced** if $\gcd(a, b) = 1$ and $b > 0$.

For example, $\frac{2}{3}$ is reduced but $\frac{4}{6}$ isn't. While $\frac{2}{-3}$ is neither in standard form nor reduced but $\frac{-2}{3} = -\frac{2}{3}$ is.

**Theorem 4.3.** *Let $\frac{a}{b}$ be a fraction, then there exists a unique reduced fraction $\frac{c}{d}$ such that $\frac{a}{b} = \frac{c}{d}$ as rational numbers.*

*Proof.* This is Problem 4.1. □

For example, $-1.56 = \frac{156}{-100} = \frac{39}{-25} = -\frac{39}{25}$.

**Proposition 4.4.** *If $x$ is a nonzero rational number, then there exist unique integer $e_2, e_3, \ldots, e_p, \ldots$ indexed by prime numbers, such that*

*(1) all but finitely many of $e_p$'s are 0.*

*(2) $x = \pm 2^{e_2} \cdot 3^{e_3} \cdots p^{e_p} \cdots$.*

*Sketch of Proof.* Write $x = \frac{a}{b}$ in reduced form, and let

$$a = \pm 2^{f_2} \cdot 3^{f_3} \cdots p^{f_p} \cdots$$

$$b = 2^{g_2} \cdot 3^{g_3} \cdots p^{g_p} \cdots$$

where $f_p, g_p \geqslant 0$. Then taking $e_p \coloneqq f_p - g_p$ gives us $x = \pm 2^{e_2} \cdot 3^{e_3} \cdots p^{e_p} \cdots$. □

For exmaple, $-1.56 = -\frac{39}{25} = -\frac{3 \cdot 13}{5^2} = -2^0 \cdot 3^1 \cdot 5^{-2} \cdot 7^0 \cdot 11^0 \cdot 13^1$

**Definition 4.5.** A complex number is **irrational** if it is not rational

For example, $\sqrt{2}$ is irrational.

More generally,

**Proposition 4.6.** *Let $a/b$ be a reduced fraction and let $n \geqslant 2$ be an integer. Then $\alpha = \sqrt[n]{a/b}$ is a rational number if and only if $a$ and $b$ are $n^{th}$ powers.*

*Proof.* ($\Rightarrow$) Suppose $\alpha$ is rational, so write $\alpha = c/d$ in reduced form, that is $\gcd(c, d) = 1$ and $d > 0$. Then

$$\frac{a}{b} = \alpha^n = \frac{c^n}{d^n}$$

Since $\gcd(c, d) = 1$, therefore $\gcd(c^n, d^n) = \gcd(c, d)^n = 1$ by Problem 2.3 and, of course, $d^n > 0$ since $d > 0$. Hence $c^n/d^n$ is in reduced form, and thus by the uniqueness statement in Theorem 4.3 we get $a = c^n$ and $b = d^n$.

($\Leftarrow$) If $a$ and $b$ are $n^{\text{th}}$ powers, i.e., $a = c^n$ and $b = d^n$ for some integers $c, d$. Then $\alpha = \sqrt[n]{a/b} = c/d$, and hence $\alpha$ is rational. □

**Example 4.7.**

(1) $\sqrt{18}$ is irrational. Two ways to conclude this, $18 = 2 \cdot 3^2$. For 18 to be a square, the exponents in its prime factorisation necessarily need to be even.

Alternatively, assume $18 = n^2$, then $16 < 18 = n^2 < 25$, and hence $4 < n < 5$ which isn't possible. So 18 is not a square, and so $\sqrt{18}$ is irrational.

(2) $\sqrt[4]{3/5}$ is irrational; since, as primes, 3 and 5 cannot be fourth powers.

## 4.2. Algebraic Numbers

**Definition 4.8.** A complex number $\alpha$ is said to be **algebraic** if it is a root of a polynomial with integer coefficients.

That is, there exists a polynomial $P(T) = c_d T^d + \cdots + c_1 T + c_0$, where $c_i \in \mathbb{Z}$ for $0 \leqslant i \leqslant d$ and $c_i \neq 0$ for some $1 \leqslant i \leqslant d$, such that

$$P(\alpha) = c_d \alpha^d + \cdots + c_1 \alpha + c_0 = 0.$$

If $\alpha$ is not algebraic, then we say $\alpha$ is **transcendental**.

**Example 4.9.**

(1) Rational numbers are algebraic: let $\alpha = a/b$, then $\alpha$ is a root of $P(T) = bT - a$.

(2) $\sqrt{2}$ is irrational *but* algebraic; it's a root of $P(T) = T^2 - 2$.

(3) More generally, consider $\alpha = \sqrt[n]{a/b}$ where $a/b$ is any rational number, then $\alpha$ is algebraic. Since $\alpha$ is a zero of $P(T) = bT^n - a$. For example, $-1$ is a root of $P(T) = T^2 + 1$.

(4) $2\sqrt{2} + \sqrt{3}$ is algebraic. We will show this.

**Fact.** If $\alpha$ and $\beta$ are algebraic, then

$$\alpha + \beta, \quad \alpha - \beta, \quad \alpha\beta, \quad \alpha/\beta \text{ (provided } \beta \neq 0)$$

are all also algebraic.

**Proposition 4.10.** *$2\sqrt{2} + \sqrt{3}$ is algebraic.*

*Proof.* We want to find a polynomial $P(T)$ such that $P(2\sqrt{2} + \sqrt{3}) = 0$. Consider

$$\begin{aligned}
\alpha &= 2\sqrt{2} + \sqrt{3} \\
\alpha - \sqrt{3} &= 2\sqrt{2} \\
(\alpha - \sqrt{3})^2 &= (2\sqrt{2})^2 \\
\alpha^2 - 2\sqrt{3}\alpha + 3 &= 8 \\
\alpha^2 - 5 &= 2\sqrt{3}\alpha \\
(\alpha^2 - 5)^2 &= (2\sqrt{3}\alpha)^2 \\
\alpha^4 - 10\alpha^2 + 25 &= 12\alpha^2
\end{aligned}$$

Therefore $\alpha^4 - 22\alpha^2 + 25 = 0$.

Hence, by construction, $P(T) = T^4 - 22T^2 + 25$ is such that $P(\alpha) = 0$. Thus $\alpha$ is algebraic. □

The following result can be used to conclude if an algebraic number is irrational.

**Theorem 4.11** (Rational Root Theorem)**.** *Let $a/b$ be a rational number in reduced form such that it is a root of a polynomial*

$$P(T) = c_d T^d + c_{d-1} T^{d-1} + \cdots + c_1 T + c_0$$

*where $c_i \in \mathbb{Z}$. Then $a \mid c_0$ and $b \mid c_d$.*

*Proof.* By assumption

$$P\left(\frac{a}{b}\right) = c_d \left(\frac{a}{b}\right)^d + c_{d-1}\left(\frac{a}{b}\right)^{d-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0$$

Then

$$c_d a^d + c_{d-1} a^{d-1} b + \cdots c_1 a b^{d-1} + c_0 b^d = 0$$

Therefore,

$$c_d a^d = -b(c_{d-1} a^{d-1} + \cdots + c_1 a b^{d-2}); \text{ and}$$

$$c_0 b^d = -a(c_d a^{d-1} + \cdots + c_1 b^{d-1})$$

Therefore $b \mid c_d a^d$ and $a \mid c_0 b^d$. Since $\gcd(a, b) = 1$, hence $\gcd(a, b^d) = \gcd(a^d, b) = 1$. Thus $b \mid c_d$ and $a \mid c_0$, by Lemma 2.3. □

For example, $\alpha = 2\sqrt{2} + \sqrt{3}$ is irrational. We found $P(T) = T^4 - 22T^2 + 25$ is such that $P(\alpha) = 0$. Suppose $\alpha = a/b$ is rational, then $a \mid 25$ and $b \mid 1$ by Theorem 4.11 above.

Therefore $a/b \in \{\pm 1, \pm 5, \pm 25\}$ but none of them equal $2\sqrt{2} + \sqrt{3}$. Therefore $2\sqrt{2} + \sqrt{3}$ is irrational.

**Example 4.12** (in-class)**.** $\sqrt{3} + \sqrt{5}$ is algebraic and irrational.

## 4.3. Transcendental Numbers

$\mathbb{C}$ is uncountable but the set of all algebraic numbers is countable (Problem 4.3). Therefore there are uncountably many transcendental numbers.

**Theorem 4.13** (Lindemann & Weierstrass, 1800's)**.** *$\pi$ and $e$ are transcendental.*

**Open Question D.** *Is $e + \pi$ transcendental?*

**Corollary 4.14** (ancient)**.** *We cannot square the circle. That is, using only a straight ruler and compass we cannot construct a square whose area is equal to $\pi$.*

**Example 4.15.** Let $k \geqslant 1$ be an integer, then

$$\zeta_k = 1 + \frac{1}{2^k} + \frac{1}{3^k} + \frac{1}{4^k} + \cdots \quad \text{converges when } k > 1.$$

- $\zeta_2 = \displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ (dubbed the Basel problem, solved by Euler in 1734). Therefore $\zeta_2$ is transcendental, since $\pi$ is.

  More generally, $\zeta_{2r} = (\text{rational number}) \cdot \pi^{2r}$. Similarly, $\zeta_{2r}$ is transcendental.

- $\zeta_3 = \displaystyle\sum_{n=1}^{\infty} \frac{1}{n^3}$ is irrational (proven by Apéry, 1979). We don't yet know if it is transcendental.

  **Open Question E.** *Is $\zeta_3$ transcendental?*

- The *Euler-Mascheroni constant* $\gamma = \displaystyle\lim_{n\to\infty} \left(-\ln(n) + 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n}\right)$.

  **Open Question F.** *Is $\gamma$ irrational?*

## 4.4. Diophantine Approximation & Ford Circles

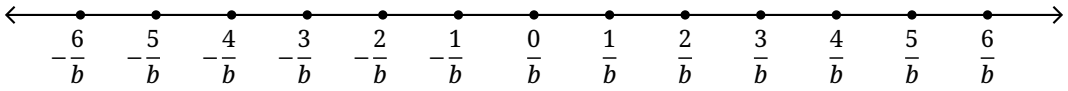
Recall that $\mathbb{Q}$ is **dense** in $\mathbb{R}$, i.e., for any $x \in \mathbb{R}$ and $\varepsilon > 0$, we can find a $q \in \mathbb{Q}$ such that $|x - q| < \varepsilon$.

How well can we approximate a real number $x$ by a rational number?

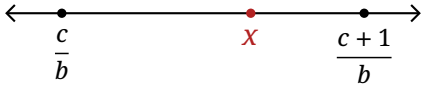
**Proposition 4.16.** *Let $x$ be any real number and $b$ a positive integer. Then there exists an integer $a$ such that*

$$\left| x - \frac{a}{b} \right| \leqslant \frac{1}{2b}$$

*Proof.* Plot $\frac{1}{b}\mathbb{Z}$




Then, say




Between $c/b$ and $(c+1)/b$, choose the one closest to $x$ and define $a/b$ as such. That is,

$$\frac{a}{b} = \begin{cases} \frac{c}{b} & \text{if } \left| x - \frac{c}{b} \right| < \left| x - \frac{c+1}{b} \right| \\ \frac{c+1}{b} & \text{if } \left| x - \frac{c+1}{b} \right| < \left| x - \frac{c}{b} \right| \end{cases}$$

So,

$$\left| x - \frac{a}{b} \right| \leqslant \frac{1}{2} \left( \text{length of } \left[ \frac{c}{b}, \frac{c+1}{b} \right] \right) = \frac{1}{2} \left( \frac{c+1}{b} - \frac{c}{b} \right) = \frac{1}{2b}$$

as claimed. □

**Remark 4.17.** The **price** of a (reduced) fraction is the size of its denominator.

For example, the fraction $314/100 = 157/50$ costs \$50. As an approximation of $\pi = 3.1415926\ldots$, we have $|\pi - 157/50| \approx 0.00159$.

But for price of \$7, we can purchase the fraction $22/7$ and as an approximation of $\pi$ we have $|\pi - 22/7| \approx 0.0013$. So, this is a better approximation for a better price!

**Diophantine approximation** studies the question: given a real number $x$, what is the relationship between the *accuracy* of a rational approximation and its *cost*.

Therefore Proposition 4.16 tells us that given \$$b$, we can approximate every real number $x$ within a distance of $1/2b$.

Recall that $|\pi - 157/50| \approx 0.00159$; compared to $1/2b = 1/100 = 0.01$, it is $\sim 16\%$ off. While comparing $|\pi - 22/7| \approx 0.0013$ with $1/2b = 1/14 \approx 0.07$, it is $\sim 2\%$ off.

Why do we care about this? This is one strategy to prove transcendence of irrational numbers.

If we were attempting to prove transcendence definitionally, for example for $\pi$ and $e$, then we would have to show that for *every* polynomial $P$ with integer coefficients, we must have $P(\pi), P(e) \neq 0$. That's a tall order, since there are infinitely such polynomials.

One idea in transcendence theory, a rule of thumb, is that if if you can approximate an irrational number $\alpha$ by rational (or algebraic) numbers very well, then $\alpha$ is likely to be transcendental.

We will now give a stronger, and historically significant, Diophantine approximation theorem.

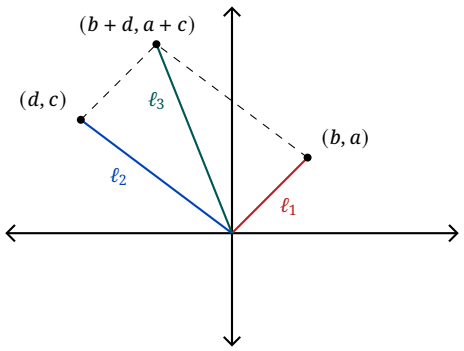
**Definition 4.18.** Let $a/b$ and $c/d$ be fractions. The **mediant** of $a/b$ and $c/d$ is

$$\frac{a}{b} \vee \frac{c}{d} \coloneqq \frac{a+c}{b+d}$$

For example, $\frac{5}{3} \vee \frac{11}{17} = \frac{5+11}{3+17} = \frac{16}{20}$.

**Proposition 4.19.** *Let $a/b$ and $c/d$ be reduced fractions, then $a/b \vee c/d$ lies between $a/b$ and $c/d$.*

*Proof.* Plot $(b, a)$ and $(d, c)$ in the Cartesian plane; say, without loss of generality, we get



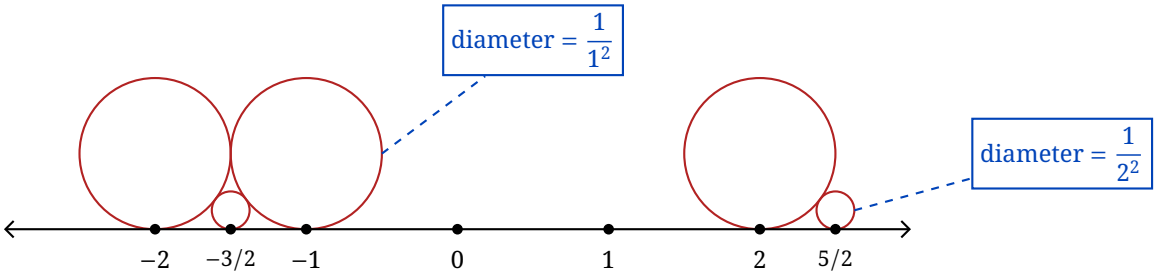

Then note that

$$\frac{a}{b} \text{ is the slope of } \ell_1, \qquad \frac{c}{d} \text{ is the slope of } \ell_2, \qquad \frac{a+c}{b+d} \text{ is the slope of } \ell_3$$

Therefore, as a rational number, $\frac{a}{b} \vee \frac{c}{d} = \frac{a+c}{b+d}$ lies between $\frac{a}{b}$ and $\frac{c}{d}$. □

**Definition 4.20.** Let $a/b$ be a fraction in standard form. The **Ford circle atop $\frac{a}{b}$** is

the circle of diameter $\frac{1}{b^2}$ that is above and tangent to the real line at the rational number $\frac{a}{b}$.




Note that some Ford circles are tangent to each other.

Ford circles are named for L.R. Ford, who first revealed the connections between the circles and Diophantine approximation (as we will soon see) in an article in 1938.

**Definition 4.21.** Let $a/b$ and $c/d$ be fractions. Then we say $\frac{a}{b}$ **kisses** $\frac{c}{d}$, denoted $\frac{a}{b} \heartsuit \frac{c}{d}$, if $ad - bc = \pm 1$.

**Proposition 4.22.** *If $a/b$ kisses any fraction $c/d$ at all, then* $\gcd(a, b) = 1$.

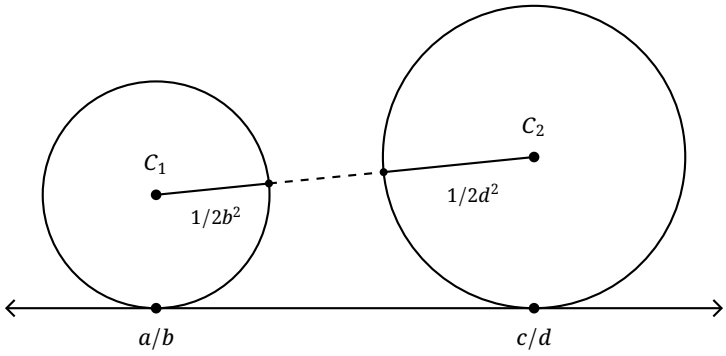
*Proof.* Assume $a/b$ kisses some fraction $c/d$, then one has $ad - bc = \pm 1$. That is, $ax + by = \pm 1$ has an integer solution: $(d, -c)$. Therefore $\gcd(a, b) \mid \pm 1$ and hence, necessarily, $\gcd(a, b) = 1$. □

Kissing fractions are an algebraic characterisation of the geometry of Ford circles.

**Theorem 4.23.** *Let $a/b$ and $c/d$ be fractions such that $b, d > 0$. Then*

$$\frac{a}{b} \heartsuit \frac{c}{d} \text{ if and only if Ford circles atop } \frac{a}{b} \text{ and } \frac{c}{d} \text{ are tangent to each other.}$$

*Proof.* Without loss of generality, consider the following schematic of the Ford circles under consideration




Here $C_1$ and $C_2$ are the centres of the Ford circles atop $a/b$ and $c/d$ respectively, and necessarily

$$\text{the cartesian coordinates of } C_1 \text{ are } = \left(\frac{a}{b}, \frac{1}{2b^2}\right); \text{ and}$$

$$\text{the cartesian coordinates of } C_2 \text{ are } = \left(\frac{c}{d}, \frac{1}{2d^2}\right)$$

We will be concerned with $\overline{C_1C_2}$, the distance of the line segment from $C_1$ to $C_2$.

Using the distance formula, we have

$$\overline{C_1C_2}^2 = \left(\frac{1}{2b^2} - \frac{1}{2d^2}\right)^2 + \left(\frac{a}{b} - \frac{c}{d}\right)^2 = \left(\frac{1}{2b^2} - \frac{1}{2d^2}\right)^2 + \left(\frac{ad-bc}{bd}\right)^2 \tag{☂}$$

Now, the Ford circles are tangent to each other if and only if $\overline{C_1C_2} = \frac{1}{2b^2} + \frac{1}{2d^2}$, or equivalently

$$\overline{C_1C_2}^2 = \left(\frac{1}{2b^2} + \frac{1}{2d^2}\right)^2 \tag{💡}$$

Equating (☂) and (💡), we have the following series of equivalent statements

$$\left(\frac{1}{2b^2} - \frac{1}{2d^2}\right)^2 + \left(\frac{ad-bc}{bd}\right)^2 = \left(\frac{1}{2b^2} + \frac{1}{2d^2}\right)^2$$

$$\left(\frac{ad-bc}{bd}\right)^2 = \left(\frac{1}{2b^2} + \frac{1}{2d^2}\right)^2 - \left(\frac{1}{2b^2} - \frac{1}{2d^2}\right)^2$$

$$\left(\frac{ad-bc}{bd}\right)^2 = 4\left(\frac{1}{2b^2}\right)\left(\frac{1}{2d^2}\right) = \frac{1}{b^2d^2}$$

$$(ad-bc)^2 = 1$$

$$ad - bc = \pm 1$$

Therefore, $\overline{C_1C_2} = \frac{1}{2b^2} + \frac{1}{2d^2}$ if and only if $ad - bc = \pm 1$.

Hence, the Ford circles atop $a/b$ and $c/d$ are tangent to each other if and only if $\frac{a}{b} \heartsuit \frac{c}{d}$. □

**Lemma 4.24.** *Suppose* $\frac{x}{y} \heartsuit \frac{z}{w}$, *then* $\left(\frac{x}{y} \vee \frac{z}{w}\right) \heartsuit \frac{x}{y}, \frac{z}{w}$.

*Proof.* We verify directly; since $x/y \heartsuit z/w$, i.e. $xy - yz = \pm 1$, note that

$$\begin{aligned} w(x+z) - z(y+w) &= xw + wz - yz - wz \\ &= xw - yz = \pm 1 \end{aligned}$$

Therefore $\frac{x}{y} \vee \frac{z}{w} = \frac{x+z}{y+z} \heartsuit \frac{z}{w}$; similarly $\left(\frac{x}{y} \vee \frac{z}{w}\right) \heartsuit \frac{x}{y}$. □

**Proposition 4.25.** *Let $a/b$ be a reduced fraction. Then*

(i) *$a/b$ kisses infinitely many fractions.*

(ii) *If $b > 1$, then there are exactly two reduced fractions $c/d$ and $c'/d'$, with $d, d' < b$ such that*

$$\frac{c}{d} \heartsuit \frac{a}{b} \heartsuit \frac{c'}{d'}, \quad \textit{where} \quad \frac{c}{d} \vee \frac{c'}{d'} = \frac{a}{b} \quad \textit{and} \quad \frac{c}{d} \heartsuit \frac{c'}{d'}$$

*Proof.* Let $a/b$ be a reduced fraction, i.e., $\gcd(a, b) = 1$ and $b > 0$.

(i) Recall from the proof of Proposition 4.22 that if $u/v$ is a reduced fraction kissing $a/b$, then by definition, $(x, y) = (v, u)$ is a solution to the equation

$$ax - by = \pm 1$$

Therefore, to prove our result, let us consider, without loss of generality, the equation $ax - by = 1$.

Since $a/b$ is reduced, we have $\gcd(a, -b) = \gcd(a, b) = 1$ and therefore we are seeking solutions to

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

By Theorem 1.19 all solutions to this equation are of the form

$$x = v_n = v_0 + bn \quad \text{and} \quad y = u_n = u_0 + an \qquad (\text{since } \operatorname{lcm}(a, -b) = -ab)$$

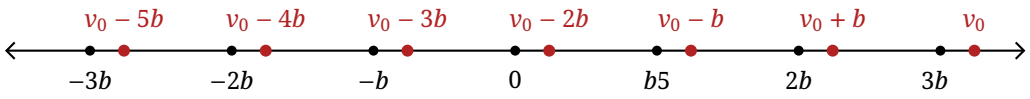
for any $n \in \mathbb{Z}$, where $(v_0, u_0)$ is a particular solution we can obtain using the division algorithm.

Since $b > 0$, note that $v_n = 0$ for at most one $n$. Whenever $v_n \neq 0$, $\frac{u_n}{v_n}$ or $\frac{-u_n}{-v_n}$ is a reduced fraction kissing $\frac{a}{b}$.

Hence, there are infinitely many fractions that kiss $a/b$. □

(ii) Assume $b > 1$ and let $u_n$, $v_n$, for any $n \in \mathbb{Z}$, be as in (i). Consider the set $\{v_n : n \in \mathbb{Z}\} = \{v_0 + bn : n \in \mathbb{Z}\}$.

Let us visualise this on the number line as follows, with respect to $b\mathbb{Z}$




Where could $v_0$ lie? Assume $v_0 = mb$ for some $m \in \mathbb{Z}$. Since $(v_0, u_0)$ is a solution to $ax + (-b)y = 1$, we have

$$1 = av_0 - bu_0 = a(mb) - bu_0 = b(am - u_0)$$

Since $am - u_0$ is an integer, we obtain that $b \mid 1$; contradicting the assumption $b > 1$. Therefore we *cannot* have $v_0 = mb$ for any $m \in \mathbb{Z}$. Hence $v_0 \in (kb, (k+1)b)$ for some integer $k$.

Define $d \coloneqq v_{-k} = v_0 - kb$, it is necessarily the *only* element of $\{v_0 + bn : n \in \mathbb{Z}\}$ in the inerval $(0, b)$.

Define $c \coloneqq u_{-k}$. Then $0 < d < b$ and, by definition, $c/d \heartsuit a/b$ with $ad - bc = 1$.

Now define $d' \coloneqq b - d$ and $c' \coloneqq a - c$. Necessarily $0 < d' = b - d < b$ and by construction

$$\frac{c}{d} \vee \frac{c'}{d'} = \frac{c + c'}{d + d'} = \frac{a}{b}$$

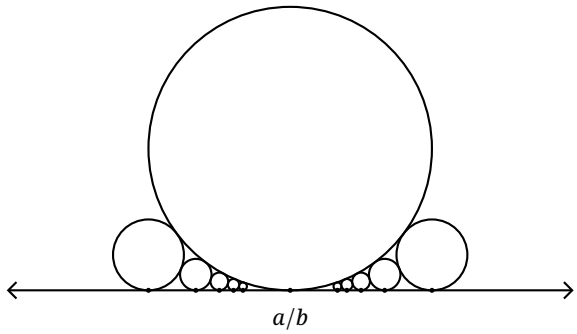
Therefore, by Lemma 4.24, we have $c'/d' \heartsuit a/b$. Finally, note that

$$cd' - c'd = c(b - d) - (a - c)d = bc - ad = -(ad - bc) = -1$$

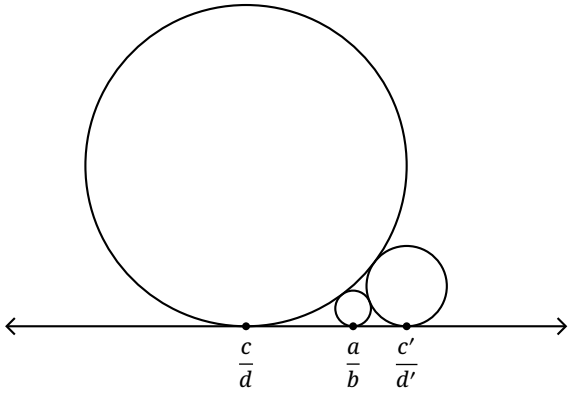
Thus, $c/d \heartsuit c'/d'$. □

**Corollary 4.26** (geometric form)**.** *Let $a/b$ be a reduced fraction. Then*

(i) *The Ford circle atop $a/b$ has infinitely many Ford circles tangent to it.*




(ii) *If $b > 1$, then among the infinitely many Ford circles as above, there are exactly two whose mediant is the Ford circle atop $a/b$.*




**Example 4.27.** Find the two kissing (reduced) fractions whose mediant is $83/71$.

*Answer.* If $x/y$ was one of them, then $x/y \heartsuit 83/71$ and so $71x - 83y = \pm 1$. Let us employ the division algorithm

$$83 = 71(1) + 12 \quad \rightsquigarrow \quad 71 = 12(5) + 11 \quad \rightsquigarrow \quad 12 = 11(1) + 1 \quad \rightsquigarrow \quad 11 = 1(11) + 0$$

Running this backwards, we get $1 = 71(-7) + 83(6)$ and so

$$-1 = 71(7) - 83(6).$$

Verifying $6 < 71$, take $\dfrac{c}{d} = \dfrac{7}{6}$ and $\dfrac{c'}{d'} = \dfrac{83 - 7}{71 - 6} = \dfrac{76}{65}$. □

**Example 4.28** (in-class)**.** Find the two kissing (reduced) fractions $a/b$ and $c/d$ whose mediant is $15/32$.

**Theorem 4.29.** *Consider the following process*

Step I. *Start with fractions $n/1$ as $n$ runs through the integers.*

Step II. *Whenever you see two kissing fractions, form their mediant.*

Step III. *Keep repeating* Step II.

*Then*

(i) *The fractions occurring in this sequence are reduced.*

(ii) *Conversely, all reduced fractions occur in this sequence.*

*Proof.* We induct on the the denominator of $a/b$, where $a/b$ is an element of the sequence.

(i) For $b = 1$, the fraction $\dfrac{a}{1}$ is reduced. Assume the inductive hypothesis.

If $\dfrac{a}{b} \heartsuit \dfrac{c}{d}$, then $\left(\dfrac{a}{b} \vee \dfrac{c}{d}\right) \heartsuit \dfrac{a}{b}$, by Lemma 4.24. Therefore the mediant is reduced by Proposition 4.22. □

(ii) If $b = 1$, then $\dfrac{a}{1}$ occurs in the base step. Assume the inductive hypothesis holds for $1 \leqslant k < b$.

For $\dfrac{a}{b}$ with $b > 1$, by Proposition 4.25, there exist reduced fractions $\dfrac{c}{d}$ and $\dfrac{c'}{d'}$ with $d, d' < b$ such that

$$\frac{c}{d} \vee \frac{c'}{d'} = \frac{a}{b}$$

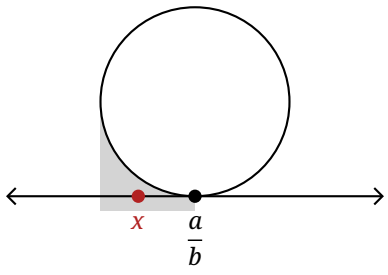
$\dfrac{c}{d}$ and $\dfrac{c'}{d'}$ occur in the sequence by the inductive hypothesis. Therefore, so does $\dfrac{a}{b}$ as their mediant. □

**Theorem 4.30** (Dirichlet's Approximation Theorem)**.** *Let $x$ be an irrational real number. Then there exist infinitely many reduced fractions $a/b$ such that*

$$\left| x - \frac{a}{b} \right| < \frac{1}{2b^2}$$

*Proof.* Let us discuss our strategy: to demonstrate the theorem, it suffices to prove that $x$ lies in the shadows of infinitely many Ford circles.

Suppose an irrational $x$ lies in the shadow of a Ford circle atop $a/b$; the Ford circle has radius $1/2b^2$. Since $x$ is irrational, necessarily $x \neq a/b$ and $x \neq a/b \pm 1/2b^2$.

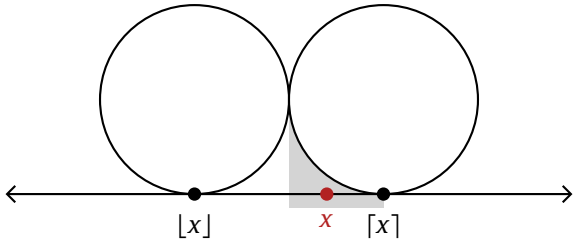



Necessarily, if $x$ lies in the shadow of a Ford circle atop $a/b$, then

$$|\, x - a/b \,| < (\text{radius of Ford circle atop } a/b) = 1/2b^2.$$

**Step I.** Assume $b = 1$. Then $x$ is in the shadow of the Ford circle atop $\dfrac{\lfloor x \rfloor}{1}$ or $\dfrac{\lceil x \rceil}{1}$.

Recall that $\lfloor x \rfloor$ is the largest integer $< x$ and $\lceil x \rceil$ is the smallest integer $> x$. Moreover, $\lceil x \rceil - \lfloor x \rfloor = 1$.

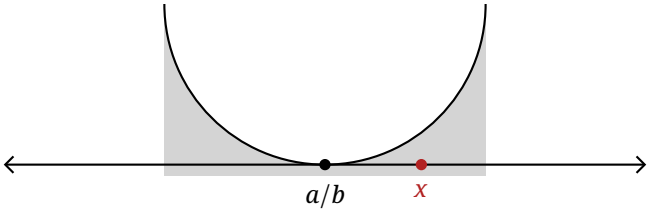



Let $a = \lfloor x \rfloor$ or $a = \lceil x \rceil$ if $x$ is in the shadow of the Ford circle atop $\frac{\lfloor x \rfloor}{1}$ or $\frac{\lceil x \rceil}{1}$ respectively. Then

$$\left| x - \frac{a}{1} \right| < (\text{radius of Ford circle atop } a/1) = \frac{1}{2}$$

**Step II.** Consider a Ford circle atop $a/b$ which shadows $x$.

Since $x$ is an irrational real number, either $x > a/b$ or $x < a/b$. Let us treat the case $x > a/b$.




**Claim.** *There exists a reduced fraction* $\frac{c}{d} > \frac{a}{b}$ *such that* $d \leqslant b$ *and* $\frac{c}{d} \heartsuit \frac{a}{b}$

*Proof of Claim.* If $b = 1$, take $\frac{c}{d} = \frac{a+1}{1}$.

If $b > 1$, then by Proposition 4.25 we can find reduced fractions $x/y$ and $x'/y'$ with $y, y' < b$ such that $a/b$ is their mediant.

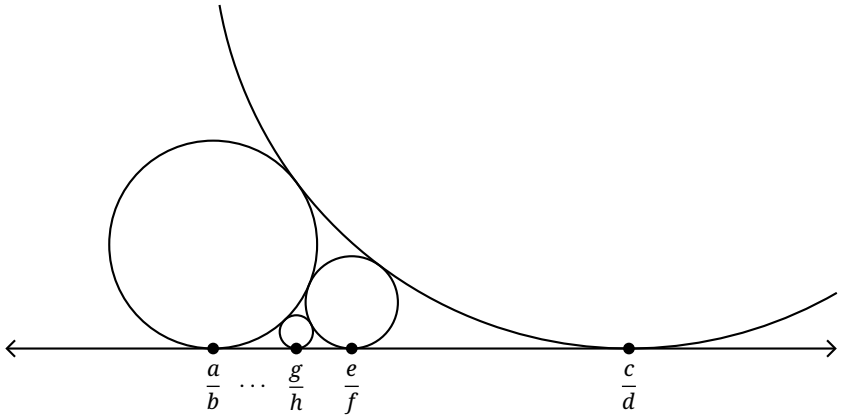
Let $c/d$ be one of these fractions that lies to the right of $a/b$ and by Lemma 4.24 we know that $c/d \heartsuit a/b$. □

Let $c/d$ be as in the claim. Consider the chain

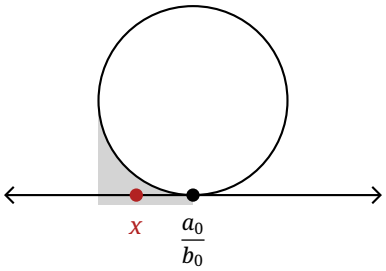
$$\frac{e}{f} = \frac{a}{b} \vee \frac{c}{d}$$

$$\frac{g}{h} = \frac{a}{b} \vee \frac{e}{f}$$

$$\vdots$$



The shadows of all these Ford circles cover the right shadow under $a/b$. So, at least one of the Ford circles in the chain must shadow $x$. Let's call the rational number this Ford circle is atop $a_0/b_0$, where $b_0 < b$.




The radius of the circle $= \frac{1}{2}(\text{diameter}) = \frac{1}{2b_0^2}$. So,

$$\left| x - \frac{a_0}{b_0} \right| < \frac{1}{2b_0^2}$$

The case $x < a/b$ is similar (everything happens on the left).

The theorem follows by starting with **Step I** and repeatedly applying **Step II**. □

**Warning** Theorem 4.30 does not imply that this approximation works for *every* integer $b$.

For example, consider $\pi = 3.1415926\ldots$. For $b = 1$, we have $|\pi - 3| < \frac{1}{2}$.

For $b = 2$, we cannot find an $\frac{a}{2}$ such that $\left|\pi - \frac{a}{2}\right| < \frac{1}{2 \cdot 2^2}$.

Because the smallest fraction of this form is $\frac{7}{2} = 3.5$ and $|\pi - 3.5| \approx 0.36$ while $\frac{1}{2 \cdot 2^2} = 0.125$.

But $b = 7$ works, take $\frac{a}{b} = \frac{22}{7}$. In this way, there are infinitely such $b$'s.

**Remark 4.31.** There are two ways to improve Dirichlet's Approximation Theorem (Theorem 4.30): by increasing the constant 2 or by increasing the exponent 2.

Hurwitz (1891) and Ford (1938), independently, improved the constant from 2 to the best possible $\sqrt{5} \approx 2.236 > 2$:

$$\left| x - \frac{a}{b} \right| \leqslant \frac{1}{\sqrt{5}b^2}, \quad \text{for infinitely many rational numbers } \frac{a}{b}$$

Improving the exponent in this estimate is more difficult. A series of results, beginning with Liouville (1844), through results of Thue and Siegel, culminated with Roth's proof (1955) that the exponent cannot be improved for *algebraic* numbers:

**Theorem 4.32** (Thue–Siegel–Roth Theorem). *Let $x$ be an algebraic irrational number. Then for any positive number $\varepsilon$ and constant $C$, the inequality*

$$\left| x - \frac{a}{b} \right| < \frac{C}{b^{2+\varepsilon}}$$

*is only satisfied for finitely many fractions $\frac{a}{b}$.*

In other words, one cannot improve the exponent, even slightly, from 2 to $2 + \varepsilon$, at least not for algebraic numbers.

This gives an effective way of proving transcendence of some numbers – if it is possible to approximate an irrational number extremely well by infinitely many rational numbers, then it must be transcendental!

## Problems

**Problem 4.1.** Prove Theorem 4.3.

**Problem 4.2.**

(a) Let $a$ and $b$ be rational numbers such that $a + b\sqrt{2} = 0$. Prove that we necessarily have $a = 0$ and $b = 0$.

(In terms of linear algebra: 1 and $\sqrt{2}$ are $\mathbb{Q}$-linearly independent.)

(b) Prove that there exist no rational numbers $a$ and $b$ such that $a + b\sqrt{2} = \sqrt{3}$.

Hint: start with squaring the purported equation.

(c) Prove that there exist no rational numbers $a,\ b$ and $c$ such that $a + b\sqrt{2} + c\sqrt{3} = \sqrt{6}$.

Hint: write $a + b\sqrt{2} = \sqrt{6} - c\sqrt{3}$ and use this to isolate $\sqrt{3}$ as a fraction of terms with $\sqrt{2}$, rationalise the denominator and use (b)

(d) Prove that there exist no rational numbers $a,\ b,\ c$ such that $a + b\sqrt{2} + c\sqrt{3} = \sqrt{5}$.

(e) **(challenge)** Prove that there exist no rational numbers $a,\ b,\ c$ and $d$ such that $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = \sqrt{5}$.

**Problem 4.3.** The aim of this problem is to prove that $\mathbb{Q}^{\text{alg}}$, the set of all algebraic numbers, is countable. A set $S$ is said to be countable, if there exists an injective function $f : S \to \mathbb{N}$.

(a) Prove that a countable union of countable sets is countable.

(b) Assuming $\mathbb{Q}$ is countable, prove $\mathbb{Q}^n$ is countable, for any natural number $n$.

(c) Let $P_n$ be the set of all polynomials of degree $n$ with rational coefficients, prove $P_n$ is countable.

(d) Consider

$$R_n \coloneqq \bigcup_{p(x)\in P_n} \{\alpha \in \mathbb{C} \ :\ p(\alpha) = 0\}$$

Prove that $R_n$ is countable. Why is $R_n$ infinite?

(e) Conclude that the set of algebraic numbers is countable.

**Problem 4.4.**

(a) Find a nonzero rational polynomial $P(T)$ that has $\sqrt{5} + \sqrt[3]{7}$ as a root.

(b) Prove that $\sqrt{5} + \sqrt[3]{7}$ is irrational.

(c) Prove that if $p$ and $q$ are distinct prime numbers, then $\sqrt{p} + \sqrt{q}$ is irrational.

**Problem 4.5.** Using the Taylor expansion of $e^x$, we obtain

$$e = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} + \cdots$$

In this problem, you will prove that $e$ is irrational.

(a) Let $s_n \coloneqq \sum_{k=0}^{n} \frac{1}{k!}$, the $n^{\text{th}}$ term of the sequence of partial sums. Prove that $0 \leqslant e - s_n \leqslant \frac{1}{n} \cdot \frac{1}{n!}$

(b) Assume $e$ is rational, and say $e = p/q$. Apply the previous result to $n = q$ and arrive at a contradiction.

**Problem 4.6.** Using Problem 3.5, prove that for all positive integers $n$, we have

$$\sigma_1(n) \leqslant n \ln(n+1) + \gamma n;$$

where $\gamma$ is the Euler-Mascheroni constant.

**Problem 4.7.** Consider the so-called *Fibonacci sequence*, define recursively by

$$F_0 = 0,\ F_1 = 1 \text{ and } F_n = F_{n-1} + F_{n-2} \text{ for all } n \geqslant 2;$$

so the first few terms are 0, 1, 1, 2, 3, 5, 8, 13, ...

For all $n \geqslant 2$, define $r_n = F_n/F_{n-1}$; so the first few terms of the sequence $(r_n)_{n\in\mathbb{N}}$ are $\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \ldots$.

(a) Prove that for all $n \geqslant 4$, $r_n = r_{n-1} \vee r_{n-2}$.

(b) Prove that the sequence $r_n$ converges.

(c) Prove that $r_n$ converges to the *golden ratio*: $\varphi = \dfrac{1+\sqrt{5}}{2}$

(d) While proving (c), you probably will have also have proven that $\varphi$ is algebraic. Give the polynomial with integer coefficients that $\varphi$ is a root of.

For this problem, you can use any result that you may have seen in your Calculus classes.

**Note.** *This is an example of problematic naming in Number Theory. Fibonacci a.k.a. Leonardo Bonacci* introduced *this sequence to the West in the 13th century but this sequence had been described earlier, for example, by Indian mathematicians, such as Pingala, as early as 200 BCE.*

**Problem 4.8.** Write a formula which describes all fractions that kiss 7/11.

**Problem 4.9.** In this problem, you will recreate Dirichlet's proof of his eponymous approximation theorem (Theorem 4.30) from circa 1840. This is slightly weaker than our result using Ford circles, but strong than the naive bound (Proposition 4.16).

Let $x$ be a real number, and let $n$ be a positive integer.

(a) For each integer $b$ between 1 and $n$, let $r_b = bx - \lfloor bx \rfloor$. The set $S = \{0, r_1, r_2, \ldots, r_n, 1\}$ contains $n+2$ real numbers between 0 and 1. Prove that there are elements $s, t \in S$ such that

$$0 < t - s \leqslant \frac{1}{n+1}$$

(b) Prove that there exist integers $a,\ b$ such that $1 \leqslant b \leqslant n$ and

$$|\, bx - a \,| \leqslant \frac{1}{n+1}$$

Hint: consider the previous part. Three cases are needed: $s = 0,$, $t = r_b$ (or) $s = r_b,\ t = 1$ (or) $s = r_b,\ t = r_c$.

(c) Prove that if $|\, bx - a \,| \leqslant \dfrac{1}{n+1}$ and $b \leqslant n$, then

$$\left| x - \frac{a}{b} \right| < \frac{1}{b^2}$$

Conclude that if $x$ is a real number, there exist infinitely fractions $a/b$ satifying the above inequality.

**Problem 4.10.** Use the Thue–Siegel–Roth theorem (Theorem 4.32) to prove that there are only finitely many integer solutions $(x, y)$ to the equation

$$x^3 - 5y^3 = 100$$

Hint: Use linear approximation at $x = 5$ to prove that

$$\left| \sqrt[3]{5+x} - \sqrt[3]{5} \right| < \frac{1}{3}\, 5^{-2/3} x$$

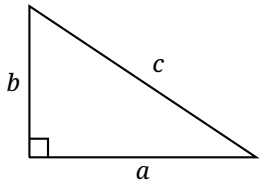
when $x > 0$. Use this to show that if $(a, b)$ is any solution to the equation, then $a/b$ is very close to $\sqrt[3]{5}$.

# 5. Towards Quadratic Diophantine Equations

We continue our investigation of Diophantine equations and focus now on quadratic Diophantine equations. The simplest one leads us to the following classical consideration.

## 5.1. Pythagorean Triples

**Definition 5.1.** Let $a, b, c$ be positive integers. Say $(a, b, c)$ is a **Pythagorean triple** if $a^2 + b^2 = c^2$.




For example, $(3, 4, 5)$, $(5, 12, 13)$ etc.

Call a Pythagorean triple $(a, b, c)$ **primitive** if $\gcd(a, b, c) = 1$. For example, $(3, 4, 5)$ is primitive but $(6, 8, 10)$ is not.

Observe that a Pythagorean triple is precisely an integer solution to the Diophantine equation $X^2 + Y^2 = Z^2$.

Our **goal** is to *classify all* Pythagorean triples. For this, we employ a **geometric** strategy.

Start with equation

$$a^2 + b^2 = c^2$$

Since $c > 0$, we may divide both sides by $c^2$ to obtain

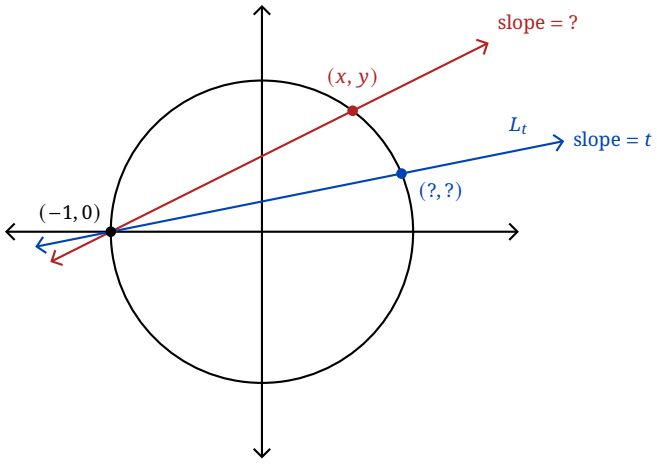
$$x^2 + y^2 = 1, \qquad \text{where } x = \frac{a}{c},\ y = \frac{b}{c}$$

Since $a, b, c$ are positive integers, $x, y$ are rational and $(x, y)$ lies on the unit circle! Denote the unit circle as $\mathsf{C}$.

In other words, any (primitive) Pythagorean triple, (primitive) integer solution to $X^2 + Y^2 = Z^2$, gives rise to a rational point (points with rational coordinates) on $\mathsf{C}$, rational solution to $x^2 + y^2 = 1$.

Therefore, our **new goal** is to *classify all* rational points on $\mathsf{C} : x^2 + y^2 = 1$.

For a rational point $(x, y)$ on $\mathsf{C}$, consider the line passing through $(x, y)$ and $(-1, 0)$, a fixed rational point on $\mathsf{C}$. What can you say about the slope of this line?




On the other hand, suppose we draw a line $L_t$ through $(-1, 0)$, a fixed rational point on $\mathsf{C}$, with rational slop $t$, what we can say about the point at which it intersects $\mathsf{C}$?

**Proposition 5.2.** *There's a bijection, where* $P_0 = (-1, 0)$

$$\left\{ P = (x, y) \in \mathbb{Q}^2 \ : \ \begin{array}{c} P \neq P_0 \\ x^2 + y^2 = 1 \end{array} \right\} \underset{g}{\overset{f}{\rightleftarrows}} \left\{ \begin{array}{c} \textit{lines through } P_0 \textit{ with} \\ \textit{rational slope } t \end{array} \right\} \xleftrightarrow{\text{via } t} \mathbb{Q}$$

*Proof.* Define the function

$$f : P \mapsto \text{the line } L \text{ passing through } P_0 \text{ and } P = (x, y)$$

Let us show that this map is well-defined by exhibiting that $L$ indeed as a rational slope. The slope of $L$ is

$$\frac{y - 0}{x - (-1)} = \frac{y}{x + 1}$$

is rational since $x, y$ are rational numbers.

Let $L_t$ be the line passing through $P_0$ with rational slope $t$; define now the function

$$g : L_t \mapsto \text{the point of intersection } (x_t, y_t) \neq (-1, 0) \text{ of } L_t \text{ and } \mathsf{C}$$

Let us show that this map is well-defined by exhibiting that $(x_t, y_t)$ is such that it has rational coordinates.

$$L_t : y = t(x - (-1)) = t(x + 1).$$

Let $(u, v)$ be a point of intersection of $L_t$ and $\mathsf{C}$, i.e., $(u, v) = (-1, 0)$ or $(x_t, y_t)$. Therefore, we have

$$v = t(u + 1) \quad \text{and} \quad u^2 + v^2 = 1$$

Substituting, we get

$$\begin{aligned} u^2 + (t(u + 1))^2 &= 1 \\ u^2 + t^2(u^2 + 2u + 1) &= 1 \\ (1 + t^2)u^2 + 2ut^2 + (u^2 - 1) &= 0 \\ u^2 + \left(\frac{2t^2}{1 + t^2}\right) u + \left(\frac{t^2 - 1}{1 + t^2}\right) &= 0 \end{aligned}$$

Observe that, by assumption, $u = -1$ or $v = x_t$, i.e., we know the roots of the quadratic equation in $u$ above. Therefore, our quadratic equation necessarily factors as follows

$$u^2 + \left(\frac{2t^2}{1 + t^2}\right) u + \left(\frac{t^2 - 1}{1 + t^2}\right) = (u - x_t)(u - (-1)) = u^2 - (x_t - 1)u - x_t$$

Comparing the constant terms of the quadratics allows us to conclude that

$$x_t = \frac{1 - t^2}{1 + t^2} \quad \text{and} \quad y_t = t(x_t + 1) = t\left(\frac{1 - t^2}{1 + t^2} + 1\right) = \frac{2t}{1 + t^2}$$

Since $t$ is rational, necessarily $(x_t, y_t) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right) \in \mathbb{Q}^2$.

One can readily check that $f$ and $g$ are inverses of each other.

In summary, every rational point $(x, y) \neq (-1, 0)$ on $\mathsf{C}$ is such that

$$(x, y) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right) \quad \text{for some } t \in \mathbb{Q}.$$

□

**Example 5.3.** The rational number $t = 1/5$ corresponds to the Pythagorean triple $(12, 5, 13)$.

$$g(L_{1/5}) = \left(\frac{1-(1/5)^2}{1+(1/5)^2}, \frac{2(1/5)}{1+(1/5)^2}\right) = \left(\frac{24}{26}, \frac{10}{26}\right) = \left(\frac{12}{13}, \frac{5}{13}\right)$$

**Remark 5.4.** Let $(a, b, c)$ be a primitive Pythagorean triple, then $P_{a,b,c} := \left(\frac{a}{c}, \frac{b}{c}\right)$ is a rational point on C.

By Proposition 5.2,

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

for a rational number $t$, which is the slope of the line through $(-1, 0)$ and $P_{a,b,c}$.

Assume $a < b$, without loss of generality, then since $a,\ b,\ c > 0$, the point $P_{a,b,c}$ lies in the first quadrant above the $y = x$ line. Therefore, we obtain $0 < t < 1$.

Write $t = q/p$ as a reduced fraction; in particular, $p > q$. Substituting, one gets

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \left(\frac{p^2-q^2}{p^2+q^2}, \frac{2pq}{p^2+q^2}\right)$$

Primitivity of the Pythagorean triple $(a, b, c)$ implies $\frac{a}{c}$ and $\frac{b}{c}$ are reduced (Problem 5.1).

If $p$ and $q$ are not both odd, then $\frac{p^2-q^2}{p^2+q^2}$ and $\frac{2pq}{p^2+q^2}$ are reduced (Problem 5.1), and therefore by Theorem 4.3

$$a = p^2 - q^2, \quad b = 2pq, \quad c = p^2 + q^2$$

If $p$ and $q$ are both odd, then $r = \frac{p+q}{2}$ and $s = \frac{p-q}{2}$ are coprime and are not both odd, and

$$\frac{p^2-q^2}{p^2+q^2} = \frac{r^2-s^2}{r^2+s^2} \quad \text{and} \quad \frac{2pq}{p^2+q^2} = \frac{2rs}{r^2+s^2}$$

The latter are reduced, by the exact same argument as the previous case, and we can conclude by Theorem 4.3

$$a = r^2 - s^2, \quad b = 2rs, \quad c = r^2 + s^2$$

In summary, given a primitive Pythagorean triple $(a, b, c)$, there exist coprime integers $m,\ n$ which have opposite **parity** with $m > n$, such that

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2$$

Conversely, the triple $(m^2 - n^2,\ 2mn,\ m^2 + n^2)$, where $m$ and $n$ are coprime integers with opposite parity, is a primitive Pythagorean triple.

This finishes are goal to classify all Pythagorean triples.

**Example 5.5.** Consider $m = 12$ and $n = 7$. Then $a = m^2 - n^2 = 95$, $b = 2mn = 168$ and $c = m^2 + n^2 = 193$. This triple $(95, 168, 193)$ is a primitive Pythagorean triple.

**Remark 5.6.** Pythagorean triples appear as soon as there is a right-angled triangles and so they have been known since antiquity. For example, in the construction of altars in Vedic India. Many authors have suggested that a Babylonian tablet, *Plimpton 322*, is a table of Pythagorean triples. In Lemma 1 before Proposition X.29 of the *Elements*, Euclid gives the recipe to produce Pythagorean triples that we discussed in Remark 5.4.

## PROBLEMS

**Problem 5.1.**

(a) Assume $(a, b, c)$ is a primitive Pythagorean triple. Prove that $\gcd(a, c) = \gcd(b, c) = 1$

(b) Assume $m, n$ are coprime integers with opposite parity. Prove that

$$\gcd(m^2 - n^2,\ m^2 + n^2) = \gcd(2mn,\ m^2 + n^2) = 1.$$

(c) Assume $p, q$ are coprime integers that are both odd.

Prove that $r = \dfrac{p+q}{2}$, $s = \dfrac{p-q}{2}$ are coprime with opposite parity; moreover,

$$\frac{p^2 - q^2}{p^2 + q^2} = \frac{r^2 - s^2}{r^2 + s^2} \quad \text{and} \quad \frac{2pq}{p^2 + q^2} = \frac{2rs}{r^2 + s^2}$$

(d) Assume $m$ and $n$ are integers. Show that $(m^2 - n^2,\ 2mn,\ m^2 + n^2)$ is a Pythagorean triple.

**Problem 5.2.** There exist other proofs for the result we obtained in Remark 5.4, you will explore one relying more directly on ideas from previous chapters below.

Let $(a, b, c)$ be a primitive Pythagorean triple.

(a) Use Lemma 6.9 to argue that $a$ and $b$ cannot both be even.

(b) Use primitivity of the triple $(a, b, c)$ to argue $a$ and $b$ cannot both be odd.

(c) From (a) and (b), we conclude that $a$ and $b$ have opposite parity. Prove that this implies $c$ is odd.

(d) Use primitivity of the triple $(a, b, c)$ to argue that $c$ and $a$ are coprime.

In summary, for a primitive Pythagorean triple $(a, b, c)$, we have that $a$ and $b$ have opposite parity and $c$ is odd. Assume now, without loss of generality, that $b$ is even, and so $a$ and $c$ are coprime odd integers. Write

$$b^2 = c^2 - a^2 = (c - a)(c + a)$$

Dividing by 4, we obtain

$$\left(\frac{b}{2}\right)^2 = \left(\frac{c-a}{2}\right)\left(\frac{c+a}{2}\right) \tag{✎}$$

With (c), (d), and Problem 5.1 (c), we obtain $\dfrac{c-a}{2}$ and $\dfrac{c+a}{2}$ are coprime.

(e) Let $x, y, z$ be positive integers with $\gcd(x, y) = 1$. Prove that if $xy = z^2$, then $x$ and $y$ are both perfect squares.

Hint: use prime factorisations of $x, y, z$ in your argument

(f) Apply (e) to (✎) to conclude: there exist positive integers $k$ and $\ell$ of opposite parity such that

$$a = k^2 - \ell^2,\ b = 2k\ell,\ c = k^2 + \ell^2$$

**Problem 5.3.** In Proposition 5.2 we obtained the bijection

$$\mathbb{Q} \longleftrightarrow \left\{ (x, y) \in \mathbb{Q}^2 \ : \ \begin{array}{c} (x, y) \neq P_0 = (-1, 0) \\ x^2 + y^2 = 1 \end{array} \right\}$$

where a rational number $t$ is considered to be the slope of a line through a fixed rational point $P_0 = (-1, 0)$ on $\mathsf{C}$, and the corresponding rational point is the other point of intersection of $L_t$ and $\mathsf{C}$.

More precisely, we have the following

$$\mathbb{Q} \longleftrightarrow \left\{ (x,y) \in \mathbb{Q}^2 \ : \ \begin{array}{c} (x,y) \neq P_0 = (-1,0) \\ x^2 + y^2 = 1 \end{array} \right\}$$

$$t \longmapsto \left( \frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right)$$

$$\frac{y}{x+1} \longmapsto\!\shortmid\ (x,y)$$

This is called a **rational parametrisation** of the unit circle.

Mimic the following recipe

1. Fix an explicit rational point $P_0$ on your curve. For example, for C, it was $P_0 = (-1, 0)$.
2. Take a rational number $t$, and consider the line with $t$ as its slope. Consider its points of intersections with your curve. One of them is $P_0$, show that there is only one other point of intersection and describe the coordinates of that point in terms of $t$.
3. Conversely, given a point $(x, y) \neq P_0$ on your curve, find the slope of the line given by $(x, y)$ and $P_0$.

to obtain rational parametrisations for the following curves:

(a) The *Pell-Fermat hyperbola* $x^2 - by^2 = 1$, where $b$ is a fixed constant positive integer.

(b) The *ordinary cuspidal cubic* $y^2 = x^3$.

(c) The *nodal cubic* $y^2 = x^3 + x^2$.

(d) **(challenge)** The *cissoid of Diocles* $y^2(a + x) = (a - x)^3$, where $a$ is a fixed constant rational number.

This curve was considered by Greek geometer Diocles around 180 B.C.E. in the book *On Burning-Glasses* (available to us through a 15th century Arabic translation of the lost original).

**Problem 5.4.** Prove that there are infinitely many positive integer triples $(x, y, z)$ such that

$$x^2 + 2y^2 = 3z^2.$$

Hint: mimic the strategy of this section, specifically Proposition 5.2 and the set-up preceding it

# 6. Modular Arithmetic

Our aim is to still find either integer or rational solutions to Diophantine equations. A tool in our tool belt that we haven't fully explored yet are *remainders*.

Consider the following examples; observe that the last digit of a number is the remainder when divided by 10.

(1) Is $317 \times 694 = 219996$?

*No, since the last digit should be* 8. *In fact,* $317 \times 694 = 219998$.

(2) Is 9217 a square of an integer? Equivalently, does $x^2 = 9217$ have an integer solution?

*No, because the last digit of a square can only be* $0, 1, 4, 5, 6$ *or* 9.

(3) Does the equation

$$x^2 + y^2 = 1234567 \tag{ϟ}$$

have an integer solution? *We will see that we can answer this question by exploring remainders!*

## 6.1. Congruence Modulo $m$

**Definition 6.1.** Let $m$ be a positive integer, called a **modulus**.

Say that two integers $a$ and $b$ are **congruent modulo $m$**, written as $a \equiv b \bmod m$, if

$$m \mid (a - b)$$

**Important** Congruence modulo $m$ is an equivalence relation (Problem 6.1).

For example, $317 \equiv 17 \equiv 7 \equiv -3 \bmod 10$

**Remark 6.2.** Let $m$ be a modulus, and $a$ and $b$ integers.

If $a \equiv b \bmod m$, then $m \mid (a - b)$. Therefore, $a - b = mk$ for some integer $k$. Or equivalently, $a = b + mk$.

Furthemore, observe that, $a \equiv 0 \bmod m$ is equivalent to $m \mid a$.

**Proposition 6.3.** *Let $m$ be a modulus, and $a, b, c, d$ be integers such that $a \equiv b \bmod m$ and $c \equiv d \bmod m$. Then*

$$a + c \equiv b + d \bmod m \quad \textit{and} \quad ac \equiv bd \bmod m.$$

*Proof.* The statement involving the sum is Problem 6.2. Let us focus on the statement involving the product.

By assumption,

$$a - b = mr, \quad \text{for some } r \in \mathbb{Z};$$
$$c - d = ms, \quad \text{for some } s \in \mathbb{Z}$$

Therefore $a = b + mr$ and $c = d + ms$. Hence,

$$\begin{aligned} ac &= (b + mr)(d + ms) \\ &= bd + m^2rs + m(dr + bs) \end{aligned}$$

Subtracting $bc$ gives us

$$\begin{aligned} ac - bd &= m^2rs + m(dr + bs) \\ &= m(mrs + dr + bs) \end{aligned}$$

Since $mrs + dr + bs$ is an integer, therefore $m \mid (ac - bd)$. Hence $ac \equiv bd \bmod m$. □

**Definition 6.4.** Let $x$ be an integer and $m$ a modulus.

The **natural representative of $x$ modulo $m$**, denoted $[x]_m$, is the remainder $r$ left under the division lemma

$$x = mq + r, \quad 0 \leqslant r < m.$$

In particular, $x \equiv [x]_m = r \bmod m$.

That is, $[x]_m$ is the unique integer $\equiv x \bmod m$ in the interval $[0, m)$.

For example, $[9]_2 = 1$, $[317]_{10} = 7$ and $[27]_5 = 2$.

**Remark 6.5.** Rephrasing Proposition 6.3 in terms of natural representatives: for modulus $m$ and integers $a, b, c, d$

$$[a]_m + [b]_m = [a+b]_m \quad \text{and} \quad [a]_m \cdot [b]_m = [a \cdot b]_m$$

**Example 6.6.**

(1) Compute the natural representative modulo 10 of $1234567 \cdot 314159265$.

*Harder method:* Multiply this number and find out.

*Easier method:* Using Proposition 6.3,

$$\begin{aligned} 1234567 \cdot 314159265 &\equiv 7 \cdot 5 \bmod 10 \\ &= 35 \bmod 10 \\ &\equiv 5 \bmod 10 \end{aligned}$$

(2) Compute the natural representative modulo 13 of $24^5$.

First, observe that $24 = 13 + 11 \equiv 11 \bmod 13 \equiv -2 \bmod 13$. Now, by Proposition 6.3,

$$\begin{aligned} 28^5 \equiv (-2)^5 \bmod 13 &\equiv -32 \bmod 13 \\ &\equiv 39 - 32 \bmod 13 \\ &\equiv 7 \bmod 13 \end{aligned}$$

(3) Compute the natural representative of $2^{10}$ modulo 7.

**(Attempt)** $10 = 7 + 3 \equiv 3 \bmod 7$, and so

$$2^{10} \equiv 2^3 \bmod 7 \equiv 8 \bmod 7 \equiv 1 \bmod 7$$

Incorrect! $2^{10} \not\equiv 2^3 \bmod 7$.

**(Actual)** We first note that

$$2 \equiv 2 \bmod 7, \quad 2^2 \equiv 4 \bmod 7, \quad 2^3 \equiv 8 \equiv 1 \bmod 7.$$

Therefore,

$$2^{10} = 2^3 \cdot 2^3 \cdot 2^3 \cdot 2 \equiv 1 \cdot 1 \cdot 1 \cdot 2 = 2 \bmod 7$$

**Warning** In general, $b \equiv c \bmod m$ does *not* imply $a^b \equiv a^c \bmod m$.

Later in the course, we will answer: for what integer $\boxed{?}$ do we have $b \equiv c \bmod \boxed{?} \Rightarrow a^b \equiv a^c \bmod m$.

**Proposition 6.7** (Divisibility Rule for 3)**.** *Let $N$ be a positive integer, and $S$ be the sum of its digits. Then $N \equiv S \bmod 9$, and hence also $N \equiv S \bmod 3$. In particular, if $S \equiv 0 \bmod 3$, then $3 \mid N$.*

*Proof.* Let $N$ be a positive integer, and we may write

$$N = d_0 + d_1 \cdot 10 + \cdots + d_k \cdot 10^k$$

For example, $247 = 7 + 4 \cdot 10 + 7 \cdot 100$. We have defined $S = d_0 + d_1 \cdots + d_k$. Then

$$\begin{aligned} N &= d_0 + d_1 \cdot 10 + \cdots + d_k \cdot 10^k \\ &\equiv d_0 + d_1 \cdot 1 + \cdots + d_k \cdot 1^k \bmod 9, \quad \text{by Proposition 6.3} \\ &\equiv d_0 + d_1 + \cdots + d_k \bmod 9 \\ &\equiv S \bmod 9 \end{aligned}$$

□

**Example 6.8.** Back to example (ϟ): Does the equation $x^2 + y^2 = 1234567$ have an integer solution?

*Proof.* The strategy is to look at the equation modulo 4.

> **Lemma 6.9.** *Let $n$ be any integer. Prove that $n^2$ is congruent to 0 or 1 modulo 4.*
>
> *Proof.* For an integer $n$, we have two cases: either $n$ is even or odd.
>
> If $n$ is even, then $n = 2k$ for some integer $k$, and so
>
> $$n^2 = (2k)^2 = 4k^2 \equiv 0 \bmod 4$$
>
> If $n$ is odd, then $n = 2k + 1$ for some integer $k$, and so
>
> $$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 \equiv 0 + 0 + 1 = 1 \bmod 4$$
>
> Therefore, either $n^2$ is congruent to 0 or 1 modulo 4. □

By Lemma 6.9, if a solution $(x, y)$ existed then $x^2$ and $y^2$ are congruent to 0 or 1 modulo 4, and therefore

| $x^2 \bmod 4$ | $y^2 \bmod 4$ | $x^2 + y^2 \bmod 4$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 2 |

Therefore, $x^2 + y^2$ is congruent to 0, 1 or 2 modulo 4.

But

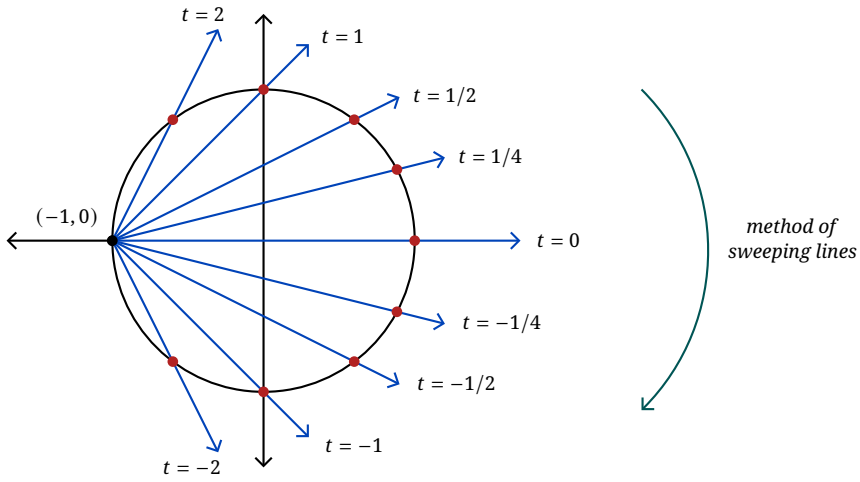
$$\begin{aligned} 1234567 &= 12345 \cdot 100 + 67 \\ &\equiv 67 \bmod 4 \\ &\equiv 64 + 3 \bmod 4 \\ &\equiv 3 \bmod 4 \end{aligned}$$

Thus, no solution exists. □

## 6.2. Solving Quadratic Diophantine Equations, so far

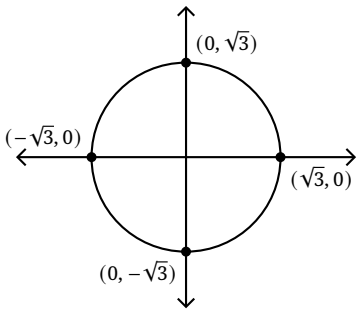
(1) $x^2 + y^2 = 1234567$ has no integer solutions.

(2) $x^2 + y^2 = z^2$ has infinitely many integer solutions, exhibited by founding all rational solutions to $X^2 + Y^2 = 1$.




(3) Find all rational solutions to $x^2 + y^2 = 3$.

(i) No obvious “pivot" with rational coordinates.




(ii) Look at integer solutions.

Since $x^2, y^2 \geqslant 0$ and $x^2 + y^2 = 3$, necessarily $0 \leqslant x^2, y^2 \leqslant 3$. So, if $x, y \in \mathbb{Z}$, then $x, y = 0, \pm 1$.

But none of these solve $x^2 + y^2 = 3$, and therefore there are no integer solutions.

Alternatively, you can reduce mod 4 and proceed as in (1).

(iii) How about rational solutions? We will show there are none.

Assume towards a contradiction that $(u, v) \in \mathbb{Q}^2$ is a solution of $x^2 + y^2 = 3$, i.e.

$$u^2 + v^2 = 3 \tag{$\circledast$}$$

Let $c$ be the lcm of the denominators of $x$ and $y$ in their reduced form, and write

$$u = \frac{a}{c}, \quad v = \frac{b}{c} \tag{$\circledast$}$$

(*e.g.*, if $u = 3/10$ and $v = 4/15$, then $c = \mathrm{lcm}(10, 15) = 30$; rewrite as $u = 9/30$ and $v = 8/30$.)

Then $c \geqslant 1$, since $u$ and $v$ are not integers (ii), and $\gcd(a, b, c) = 1$ (see Problem 6.3).

Rewriting (⩛) using (⩓), we get

$$\frac{a^2}{b^2} + \frac{b^2}{c^2} = 3 \Leftrightarrow a^2 + b^2 = 3c^2 \tag{⩦}$$

Since $a, b, c \in \mathbb{Z}$, we have

$$a^2 + b^2 \equiv 0 \bmod 3 \tag{⩔}$$

Observe that necessarily $a \equiv 0, 1, 2 \bmod 3$. Therefore,

$$a^2 \equiv \begin{cases} 0^2 = 0 \bmod 3 \\ 1^2 = 1 \bmod 3 \\ 2^2 \equiv 1 \bmod 3 \end{cases}$$

Similarly for $b^2 \bmod 3$. Hence, we may deduce that, the only way we have (⩔) is if $a^2 \equiv b^2 \equiv 0 \bmod 3$.

Thus, $3 \mid a^2$ and $3 \mid b^2$. Since 3 is a prime, we conclude $3 \mid a$ and $3 \mid b$.

Let $a = 3a_0$ and $b = 3b_0$, for some integers $a_0, b_0$. Substituting this in (⩦) gives us

$$3c^2 = (3a_0)^2 + (3b_0)^2$$

$$c^2 = 3(a_0^2 + b_0^2)$$

Therefore $3 \mid c^2$, and so necessarily $3 \mid c$.

Altogether we have $3 \mid a$, $3 \mid b$ and $3 \mid c$; but we had $\gcd(a, b, c) = 1$.

Hence we have arrived at a contradiction and thus $x^2 + y^2 = 3$ has no rational solutions.

## 6.3. Multiplicative Inverses Modulo $m$

Let $m$ be a modulus. By $\mathbb{Z}/m\mathbb{Z}$ we mean the set of equivalence classes of integers with respect to the following equivalence relation of congruence modulo $m$. For any $a \in \mathbb{Z}$, its equivalence class will be denoted as $\overline{a}$.

$$\overline{a} = \{x \in \mathbb{Z} \ : \ x \equiv a \bmod m\} = \{x \in \mathbb{Z} \ : \ x = a + mk, \text{for some integer } k\} = \{a + mk \ : \ k \in \mathbb{Z}\}$$

For example, if $m = 2,\ a = 1$, then

$$\overline{1} = \{1 + 2k \ : \ k \in \mathbb{Z}\} = \{\ldots, -3, -1, 1, 3, 5, \ldots\} = \{1 + 2n \ : \ n \in \mathbb{Z}\}$$

If $m = 5,\ a = 7$,

$$\overline{7} = \{7 + 5n \ : \ n \in \mathbb{Z}\} = \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\} = \overline{2} = \{2 + 5k \ : \ k \in \mathbb{Z}\}$$

Now, by definition, $\mathbb{Z}/m\mathbb{Z} = \left\{\overline{a} \ : \ a \in \mathbb{Z}\right\}$. Let us describe this set more concretely.

From the properties of equivalence classes, recall that if $a \equiv b \bmod m$, then $\overline{a} = \overline{b}$. In particular, $\overline{a} = \overline{[a]}_m$, where $[a]_m$ is the natural representative of $a$ modulo $m$. Now, observe that for a modulus $m$, the possibly natural representatives modulo $m$ are $0, 1, \ldots, m-1$. Therefore

$$\mathbb{Z}/m\mathbb{Z} = \left\{\overline{0},\ \overline{1},\ \ldots,\ \overline{m-1}\right\}$$

For example, $\mathbb{Z}/2\mathbb{Z} = \left\{\overline{0}, \overline{1}\right\}$ and $\mathbb{Z}/5\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\right\}$

Proposition 6.3 can be recast as saying the following addition and multiplication operations

$$\overline{a} + \overline{b} \coloneqq \overline{a + b} \quad \text{and} \quad \overline{a} \cdot \overline{b} \coloneqq \overline{ab}$$

are well-defined operations on $\mathbb{Z}/m\mathbb{Z}$.

Sometimes we may want to consider just the set of natural representatives modulo $m$, we will denote this as

$$\underline{\mathrm{R}}(m) = \{0, 1, \ldots, m-1\}$$

(1) With $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$, we can divide by any non-zero number to solve linear equations.

Consider, for example, $(2+3i)Z = 5$; then

$$\begin{aligned} Z = \frac{5}{2+3i} &= \frac{5}{2+3i} \cdot \frac{2-3i}{2-3i} \\ &= \frac{5(2-3i)}{(2+3i)(2-3i)} \\ &= \frac{10-15i}{2^2+3^2} = \frac{10}{13} - \frac{15}{13}i \end{aligned}$$

(2) With $\mathbb{Z}$, division can be tricky: $3X = 5$ has no integer solutions, but $3X = 6$ has $X = 2$ as a solution.

(3) When can we divide in $\mathbb{Z}/m\mathbb{Z}$? That is, for what $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$, is there a solution to $\overline{a}X = 1$ in $\mathbb{Z}/m\mathbb{Z}$?

**Definition 6.10.** Let $m$ be a modulus and $a \in \mathbb{Z}$. Say that $b \in \mathbb{Z}$ is a **multiplicative inverse of $a$ modulo $m$** if

$$ab \equiv 1 \bmod m$$

A multiplicative inverse of $a$ modulo $m$ is *not unique*.

For example, consider $m = 11$ and $a = 4$. Then $b = 2$ is *not* a multiplicative inverse of 4 modulo 11, since

$$ab = 8 \not\equiv 1 \bmod 11.$$

But $b = 3$ is, because $ab = 12 \equiv 1 \bmod 11$. So is $c = 14$, since $ac = 56 \equiv 1 \bmod 11$.

In fact, if $d$ is any multiplicative inverse of 4 modulo 11, then $d \equiv 3 \bmod 11$.

**Remark 6.11.** When $a$ has a multiplicative inverse $b$ modulo $m$, we can solve linear equations of the form

$$aX \equiv c \bmod m$$

Multiplying by $b$,

$$\begin{aligned} b(aX) &\equiv bc \bmod m \\ (ba)X &\equiv bc \bmod m \\ X &\equiv bc \bmod m \end{aligned}$$

since $ba \equiv 1 \bmod m$ as $b$ is a multiplicative inverse of $a$ modulo $m$.

For example, let us solve

$$4X \equiv 7 \bmod 11.$$

We found $b = 3$ is a multiplicative inverse of 4 modulo 11, therefore

$$\begin{aligned} 3(4X) &\equiv 3 \cdot 7 \bmod 11 \\ 12X &\equiv 21 \bmod 11 \\ X &\equiv 10 \bmod 11 \end{aligned}$$

So, when does a given integer have a multiplicative inverse with respect to a given modulus?

**Theorem 6.12.** *Let $m$ be a modulus and $a \in \mathbb{Z}$. Then*

(1) *$a$ has a multiplicative inverse modulo $m$ if and only if $\gcd(a, m) = 1$.*

(2) *When $a$ has a multiplicative inverse modulo $m$, then any two multiplicative inverses are necessarily congruent modulo $m$. That is, they define the same equivalence class in $\mathbb{Z}/m\mathbb{Z}$.*

*Proof.*

(1) ($\Rightarrow$) Say $b$ is the multiplicative inverse of $a$ modulo $m$, that is $ab \equiv 1 \bmod m$. Therefore $ab = 1 + mk$ for some $k \in \mathbb{Z}$. Hence $a(b) + m(-k) = 1$, and thus $\gcd(a, m) \mid 1$. Therefore, necessarily, $\gcd(a, m) = 1$.

($\Leftarrow$) Suppose $\gcd(a, m) = 1$, then by Bézout's Identity there exist $x, y \in \mathbb{Z}$ such that $ax + my = 1$. Therefore $ax \equiv 1 \bmod m$, and hence $x$ is a multiplicative inverse of $a$ modulo $m$. □

(2) Say $b$ and $b'$ are two multiplicative inverses of $a$ modulo $m$, then

$$b = b \cdot 1 \equiv b(ab') \equiv (ba)b' \equiv 1 \cdot b' \equiv b' \bmod m$$ □

**Example 6.13** (in-class)**.**

(1) Find the multiplicative inverse of 15 modulo 37.

(2) Using (1), solve the linear equation/congruence $15x \equiv 4 \bmod 37$.

**Corollary 6.14.** *$\overline{a}$ has a* **unique** *multiplicative inverse $\overline{b}$ in $\mathbb{Z}/m\mathbb{Z}$ if and only if $\gcd(a, m) = 1$.*

**Corollary 6.15** (Cancellative Property)**.** *If $\gcd(a, m) = 1$, then for any $x, y \in \mathbb{Z}$,*

$$ax \equiv ay \bmod m \Rightarrow x \equiv y \bmod m$$

**Corollary 6.16.** *Let $p$ be a prime and $a \in \mathbb{Z}$. Then $a$ has a multiplicative inverse modulo $p$ if and only if*

$$p \nmid a \text{ if and only if } \overline{a} \neq \overline{0} \text{ in } \mathbb{Z}/p\mathbb{Z}.$$

*In particular, $\mathbb{Z}/p\mathbb{Z}$ is a field!*

## Problems

**Problem 6.1.** Let $m$ be a positive integer. Prove the following properties of modular congruence:

(a) For each $a \in \mathbb{Z}$, $a \equiv a \bmod m$.

(b) If $a, b \in \mathbb{Z}$ such that $a \equiv b \bmod m$, then $b \equiv a \bmod m$.

(c) If $a, b, c \in \mathbb{Z}$ such that $a \equiv b \bmod m$ and $b \equiv c \bmod m$, then $a \equiv c \bmod m$.

**Problem 6.2.** Let $m$ be a modulus, and $a, b, c, d$ be integers such that $a \equiv b \bmod m$ and $c \equiv d \bmod m$. Prove that

$$a + c \equiv b + d \bmod m.$$

**Problem 6.3.** Consider a pair of reduced fractions, $N_u/D_u$ and $N_v/D_v$ distinct as rational numbers.

Let $c \coloneqq \operatorname{lcm}(D_u, D_v)$ and then suppose $c = D_u m_u = D_v m_v$ for some integers $m_u, m_v$.

Define $a = N_u m_u$ and $b = n_v m_v$; prove that $\gcd(a, b, c) = 1$.

**Problem 6.4.** [Divisibility Rule for 3] Let $N$ be a positive integer, and $A$ be the alternating sum of its digits. That is, if $N$ has a decimal expansion with units digit $u$, tens digit $t$, hundreds digit $h$, thousands digit $s$, then $A = u - t + h - s + \cdots$. Then $N \equiv S \bmod 11$.

In particular, if $u + h + \cdots \equiv t + s + \cdots$, then $11 \mid N$. Is 25267 divisibly by 11?

**Problem 6.5.**

(a) Let $n$ be any integer. Prove that $n^2$ is congruent to 0, 1 or 4 modulo 8.

(b) What is $1000 \bmod 8$?

(c) Prove that there exists no integer solution $(x, y, z)$ to the equation

$$x^2 + y^2 + z^2 = 31415926535897932384626433827.$$

(d) Demonstrate that there are infinitely many positive integers that *cannot* be written as a sum of three squares.

**Problem 6.6.** Let $p$ be any prime number and let $a$ and $b$ be any two integers.

(a) Prove that if $a \equiv b \bmod p$, then $a^p \equiv b^p \bmod p^2$.

(b) Prove that if $a \equiv b \bmod p$, then $a^{p^2} \equiv b^{p^2} \bmod p^3$.

(c) **(challenge)** Can you generalise?

**Problem 6.7.** Compute (the natural representative of) $3^{10^{10^{10}}} \bmod 7$.

**Problem 6.8.** Prove that a modulus $m$ is even if and only if there exists an integer $x$ such that

$$x \not\equiv 0 \bmod m \quad \text{and} x + x \equiv 0 \bmod m.$$

**Problem 6.9.** Recall the Fibonacci numbers from Problem 4.7. Prove that for all $n \geqslant 1$,

$$F_n \equiv 4^{n-1}(2^n - 1) \bmod 11$$

using mathematical induction.

**Problem 6.10.**

(a) Find the multiplicative inverse of 15 modulo 49.

(b) Using (a), solve the linear equation/congruence $15X \equiv 8 \bmod 49$.

**Problem 6.11.** Solve the congruences $5X \equiv 11 \bmod 37$ and $11Y \equiv 5 \bmod 37$. If solutions exist, find $[XY]_{37}$.

**Problem 6.12.** Fix a prime number $p$ in what follows. Let $x$ be an integer, and one can write $x = p^e m$, where $p \nmid m$. The ***p*-adic norm** of an integer $x$, denoted $|\, x \,|_p$, is defined to be

$$|\, x \,|_p \coloneqq p^{-e}$$

For example,

$$|\, 20 \,|_2 = \frac{1}{4}, \quad |\, 20 \,|_3 = 1, \quad |\, 20 \,|_5 = \frac{1}{5}$$

We define $|0|_p \coloneqq 0$. The ***p*-adic distance** between two integers $x$ and $y$ is defined to be $|\, x - y \,|_p$.

(a) Prove that $|\, -x \,|_p = |\, x \,|_p$, and $|\, xy \,|_p = |\, x \,|_p \, |\, y \,|_p$.

(b) Prove that $|\, x \,|_p \leqslant 1$ for all integers $x$, and $|\, x \,|_p = 1$ if and only if $x = \pm 1$.

(c) Prove the **ultrametric** (or **strong**) **triangle inequality**:

$$|\, x + y \,|_p \leqslant \max\{|\, x \,|_p, |\, y \,|_p\}$$

(d) Prove that (c) implies the regular triangle inequality: $|\, x + y \,|_p \leqslant |\, x \,|_p + |\, y \,|_p$.

(e) Let $a$ be an integer. Describe the set

$$B(a, p^{-e}) \coloneqq \{x \in \mathbb{Z} \,:\, |\, x - a \,|_p < p^{-e}\}$$

using the language of congruences, where $e \geqslant 0$ is also an integer.

**Problem 6.13.** We extend Problem 6.12 to $\mathbb{Q}$. Fix a prime $p$, and let $x$ be a rational number, then one can write

$$x = p^e \frac{a}{b}$$

where $p \nmid a, b$ (convince yourself) and $e \in \mathbb{Z}$. Then, similarly as the previous problem, the ***p*-adic norm** of a rational number $x$, denoted $|\, x \,|_p$, is defined to be

$$|\, x \,|_p \coloneqq p^{-e}$$

For example,

$$\left|\frac{42}{40}\right|_2 = 4, \quad \left|\frac{42}{40}\right|_3 = \frac{1}{3}, \quad \left|\frac{42}{40}\right|_5 = 5, \quad \left|\frac{42}{40}\right|_7 = \frac{1}{7}$$

The ***p*-adic distance** is similarly defined.

(a) Prove the statements (a) and (c) of Problem 6.12, where now $x$ and $y$ are rational numbers.

The ultrametric triangle inequality in this setting still implies the regular triangle inequality.

(b) Prove that the set

$$S = \{x \in \mathbb{Q} \,:\, |\, x \,|_p \leqslant 1\}$$

is closed under addition and multiplication. That is, for any $x, y \in S$, we have $xy$ and $x + y \in S$.

(c) We can explicitly describe $S$. Prove that

$$S = \left\{\frac{a}{b} \in \mathbb{Q} \,:\, a, b \in \mathbb{Z},\ p \nmid b\right\}, \qquad \text{where } a/b \text{ is understood to be reduced}$$

# 7. Modular Dynamics

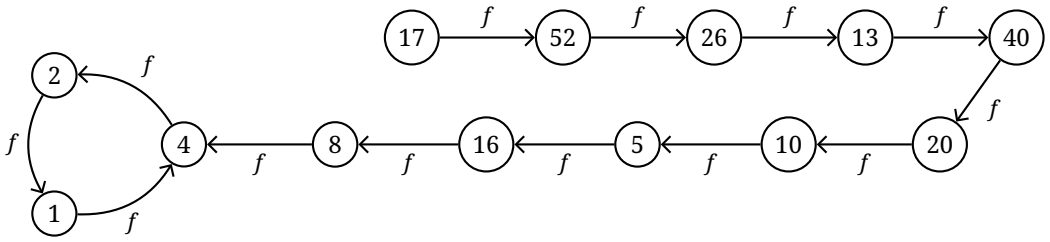
Dynamics in its simplest mathematical form (discrete time):

Let $X$ be a set and $f\colon X \to X$ a function. Pick an initial point $x_0 \in X$, what happens in this sequence

$$x_0,\ f(x_0),\ f(f(x_0)),\ f(f(f(x_0))), \ldots, f^k(x_0), \ldots ?$$

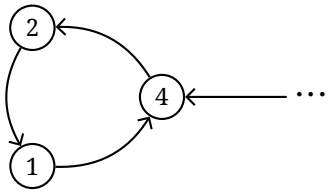
For example, consider $X = \mathbb{Z}_+ = \{1, 2, \ldots\}$, and let $f : \mathbb{Z}_+ \to \mathbb{Z}_+$ be defined as $f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ 3n+1 & \text{if } n \text{ is odd} \end{cases}$

Pick $x_0 = 17$, then the sequence reads:




**Conjecture G** (Collatz, $3n+1$). *For any $x_0 \in \mathbb{Z}_+$, there exists a $k > 0$ such that $f^k(x_0) = 1$.*

*In particular, the dynamics of $f$ eventually results in a cycle of length 3 with*



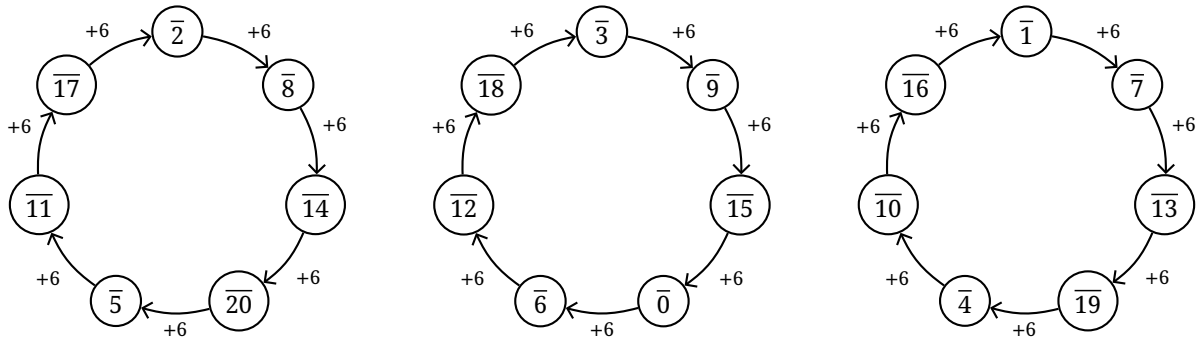

We are interested in **modular dynamics**, where either $X = \mathbb{Z}/m\mathbb{Z}$ or some subset of $\mathbb{Z}/m\mathbb{Z}$, for a modulus $m$.

## 7.1. Additive Modular Dynamics

For a modulus $m$ and $b \in \underline{\mathrm{R}}(m)$, we consider the dynamics of the function "*adding $b$ modulo $m$*"

$$\mathbf{A}_b = \mathbf{A}_{b,m}\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad \overline{x} \mapsto \overline{x+b}$$

For example, let $X = \mathbb{Z}/21\mathbb{Z}$ and consider $b = 6$. We consider the dynamics of $\mathbf{A}_6$ with $x_0 = 2, 3, 1$,




There are 3 **cycles** of **length** 7.

We can compute, in general, the number of cycles and the length of each cycle in the dynamics of $\mathbf{A}_b$ on $\mathbb{Z}/m\mathbb{Z}$.

**Proposition 7.1.** *Let $m$ be a modulus and $b \in \underline{\mathsf{R}}(m)$. Then the dynamics of $\mathbf{A}_b$ on $\mathbb{Z}/m\mathbb{Z}$ consists of $\gcd(b,m)$-many cycles of length $\ell = m/\gcd(b,m)$.*

*Proof.* Suppose we start with $\overline{x}_0 \in \mathbb{Z}/m\mathbb{Z}$

$$\overline{x}_0 \longrightarrow \overline{x_0 + b} \longrightarrow \overline{x_0 + 2b} \longrightarrow \overline{x_0 + 3b} \longrightarrow \cdots \tag{〓}$$

In step $k$, we get $\overline{x_0 + kb}$. Because $X = \mathbb{Z}/m\mathbb{Z}$ is a finite set, we return to $\overline{x}_0$ eventually (e.g., when $k = m$).

Let $\ell$ be the smallest positive integer such that

$$\overline{x}_0 = \overline{x_0 + \ell b} \tag{○}$$

and $\ell$ is necessarily the length of the cycle (〓).

Rewriting (○), we get

$$x_0 \equiv x_0 + \ell b \bmod m; \quad \text{equivalently, } \ell b \equiv 0 \bmod m$$

This gives us $m \mid \ell b$ and $\ell$ is the smallest positive integer with this property. Necessarily, $\ell b = \mathsf{lcm}(a,m)$. Thus,

$$\ell = \frac{\mathsf{lcm}(b,m)}{b} = \frac{m}{\gcd(b,m)}$$

So, the number of cycles $= \dfrac{m}{\ell} = \gcd(b,m)$. □

**Corollary 7.2.** *If $\gcd(b,m) = 1$, then $\mathbf{A}_b$ on $\mathbb{Z}/m\mathbb{Z}$ has just* **one** *cycle of length $m$.*

*Given such a $b$, we call $\overline{b}$ a* **generator** *of $\mathbb{Z}/m\mathbb{Z}$.*

## 7.2. Units Modulo *m*

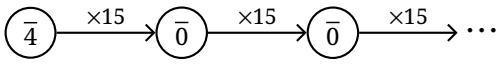
One major complication, unlike additive modular dynamics, is that the function "*multiplying $b$ modulo $m$*" is not reversible for every integer $b \in \underline{\mathsf{R}}(m)$. This results in the dynamics to not have cycles.

For example,

$$\mathbb{Z}/20\mathbb{Z} \to \mathbb{Z}/20\mathbb{Z}, \quad \overline{y} \mapsto \overline{15y}$$

is *not* reversible (bijective). Since, $15X \equiv 1 \bmod 20$ does not have a solution as $\gcd(15,20) = 5 \neq 1$.

Furthermore, e.g., with $x_0 = 4$, we have




For multiplicative dynamics, we focus on integers that have multiplicative inverses modulo $m$.

**Definition 7.3.** Let $m$ be a modulus. We define the following set

$$(\mathbb{Z}/m\mathbb{Z})^\times = \left\{\overline{u} \in \mathbb{Z}/m\mathbb{Z} \ : \ \gcd(u,m) = 1\right\};$$

The elements of $(\mathbb{Z}/m\mathbb{Z})^\times$ are called **units modulo *m***.

Sometimes we may want to consider just the set of natural representatives of integers that are multiplicatively invertible modulo $m$, we will denote this as

$$\underline{\mathsf{U}}(m) = \{y \in \mathbb{Z} \ : \ 0 \leqslant y \leqslant m, \ \gcd(y,m) = 1\}$$

For a modulus $m$ and an integer $u \in \underline{\mathsf{U}}(m)$, we consider the dynamics of the function

$$\mathbf{M}_u = \mathbf{M}_{u,m} \colon (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times, \quad \overline{y} \mapsto \overline{uy}$$

We restate the existence of multiplicative inverse modulo $m$ (Theorem 6.12)

**Proposition 7.4.** *Let $u \in \underline{R}(m)$. Then $u \in \underline{U}(m)$ if and only if $u$ has a multiplicative inverse modulo $m$ if and only if*

$$\mathbf{M}_u \colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \text{ is reversible (bijective)}$$

**Definition 7.5.** We define **Euler's totient function** $\varphi \colon \mathbb{Z}_+ \to \mathbb{C}$ as

$$\varphi(m) \coloneqq \#(\mathbb{Z}/m\mathbb{Z})^\times = \#\underline{U}(m).$$

For example, $\underline{U}(20) = \{v \in \mathbb{Z} \ : \ 0 \leqslant v \leqslant 20,\ \gcd(v, 20) = 1\} = \{1, 3, 7, 9, 11, 13, 17, 19\}$, so $\varphi(20) = 8$.

**Proposition 7.6.** *A modulus $m$ is prime if and only if $\varphi(m) = m - 1$ if and only if $\underline{U}(m) = \{1, \ldots, m-1\}$.*

*Proof.* ($\Longrightarrow$) Assume $m = p$ is prime, then necessarily

$$\underline{U}(p) = \{1, \ldots, p-1\}$$

since any positive integer $< p$ is coprime to $p$. Hence $\varphi(p) = \#\underline{U}(p) = p - 1$.

($\Longleftarrow$) Assume $\varphi(m) = m - 1$.

Necessarily $m \neq 1$. Since if we did have $m = 1$, then $m - 1 = 0$, but $\varphi(m) = \varphi(1) = \#\underline{U}(1) = \#\{0\} = 1$. Since $m \neq 1$, we may conclude that $0 \notin \underline{U}(m)$ since the only positive integer 0 is coprime to is 1; see Problem 1.3 (i).

Hence $\underline{U}(m) \subseteq \{1, \ldots, m-1\}$. Furthermore, by assumption, $\#\underline{U}(m) = \varphi(m) = m - 1 = \#\{1, \ldots, m-1\}$. Thus, we conclude that $\underline{U}(m) = \{1, \ldots, m-1\}$.

Assume for the sake of contradiction that $m$ is not prime. So, there exists an integer $u$ such that $u \mid m$ and $1 < a < m$. Since $1 < a < m$, we have $u \in \{1, \ldots, m-1\} = \underline{U}(m)$ but $u \mid m$ gives us $\gcd(a, m) = a$, by Problem 1.3 (ii). But since $u > 1$ and $u \in \underline{U}(m)$, we obtain a contradiction.

Hence, $m$ is necessarily prime. □

**Proposition 7.7.** *If $\overline{u}, \overline{v} \in (\mathbb{Z}/m\mathbb{Z})^\times$, then $\overline{u} \cdot \overline{v} = \overline{uv} \in (\mathbb{Z}/m\mathbb{Z})^\times$.*

*Therefore, $(\mathbb{Z}/m\mathbb{Z})^\times$ is closed under multiplications.*

*Proof.* Since $\overline{u}, \overline{v} \in (\mathbb{Z}/m\mathbb{Z})^\times$, by Theorem 6.12, there exist integers $u, b$ such that

$$ua \equiv 1 \bmod m \quad \text{and} \quad vb \equiv 1 \bmod m$$

Therefore,

$$(uv)(ab) = (ua)(vb) \equiv 1 \cdot 1 = 1 \bmod m$$

Hence, $ub$ is a multiplicative inverse of $uv$ and thus $\gcd(uv, m) = 1$ by Theorem 6.12. Therefore $\overline{uv} \in (\mathbb{Z}/m\mathbb{Z})^\times$. □

## 7.3. Multiplicative Modular Dynamics

For a modulus $m$ and an integer $u \in \underline{U}(m)$, we consider the dynamics of the function

$$\mathbf{M}_u = \mathbf{M}_{u,m} \colon (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times, \quad \overline{y} \mapsto \overline{uy}$$

Let's start with an example. Consider

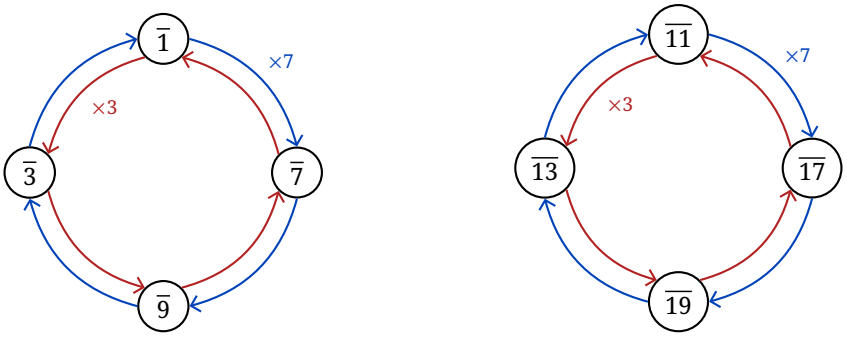
$$\mathbf{M}_7 : (\mathbb{Z}/20\mathbb{Z})^\times \to (\mathbb{Z}/20\mathbb{Z})^\times.$$

Note that

$$(\mathbb{Z}/20\mathbb{Z})^\times = \left\{\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}\right\}$$

and that 3 is the multiplicative inverse of 7 modulo 20, since $3 \cdot 7 = 21 \equiv 1 \bmod 20$.

We see that we get the following cycles




Therefore, the dynamics of $\mathbf{M}_7$ on the set $(\mathbb{Z}/20\mathbb{Z})^\times$ has 2 cycles, each of length 4.

**Lemma 7.8.** *For a modulus $m$ and an integer $u \in \underline{\mathsf{U}}(m)$. Then the dynamics of*

$$\mathbf{M}_u \colon (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$$

*consists of cycles, all of the same length.*

*Proof.* Initialising the dynamics at $\overline{1}$, we obtain a sequence of powers of $u$ modulo $m$

$$\overline{1},\ \overline{u},\ \overline{u}^2,\ \overline{u}^3,\ \ldots,\ \overline{u}^n,\ \ldots \tag{✱}$$

Since $\underline{\mathsf{U}}(m)$ is a finite set, there must be repetition.

Say, $0 \leqslant e < f$ are integers such that $u^f \equiv u^e \bmod m$. Since $\gcd(u, m) = 1$, we necessarily have $\gcd(u^e, m) = 1$; rewriting the previous expression as $u^e \cdot u^{f-e} \equiv u^e \bmod m$, by Corollary 6.15, we obtain $u^{f-e} \equiv 1 \bmod m$.

Therefore, there's an integer $\ell = f - e > 0$ such that $u^\ell \equiv 1 \bmod m$. Let $\ell_0$ be the smallest such positive integer.

> **Claim.** *If $e, f$ are integers such that $0 \leqslant e < f < \ell_0$, then $u^e \not\equiv u^f \bmod m$.*
>
> *Proof of Claim.* Suppose not, that is $e, f$ are integers as given but $u^e \equiv u^f \bmod m$. Then similarly as before, by invoking Corollary 6.15, we obtain $u^{f-e} \equiv 1 \bmod m$. This contradicts the minimality of $\ell_0$, since $f - e < \ell_0 - e < \ell_0$, therefore $u^e \not\equiv u^f \bmod m$. □

Thus, with this claim, we conclude that (✱) is a cycle of length $\ell_0$.

Now, let $\overline{y} \in \underline{\mathsf{U}}(m)$ be arbitrary, and consider the sequence

$$\overline{y},\ \overline{yu},\ \overline{y} \cdot \overline{u}^2,\ \overline{y} \cdot \overline{u}^3,\ \ldots,\ \overline{y} \cdot \overline{u}^n,\ \ldots \tag{$✱_y$}$$

Since $u^{\ell_0} \equiv 1 \bmod m$, necessarily $yu^{\ell_0} \equiv y \bmod m$. Therefore, ($✱_y$) is a cycle of length less than or equal to $\ell_0$. Suppose the length of ($✱_y$) was $k < \ell_0$, that is, $yu^k \equiv y \bmod m$. Then, since $\gcd(y, m) = 1$, by Corollary 6.15 we obtain $u^k \equiv 1 \bmod m$.

This contradicts the minimality of $\ell_0$, and hence ($✱_y$) must also have length $\ell_0$. □

**Theorem 7.9** (Euler-Fermat)**.** *Let $m$ be a modulus and $u \in \underline{\mathsf{U}}(m)$. Then*

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

*Proof.* Consider the dynamics of $\mathbf{M}_a$ on $\underline{\mathsf{U}}(m)$. We have seen in Lemma 7.8 that all cycles have the same length, say $\ell_0$. In particular, initialising at $\overline{1}$ we obtain

$$u^{\ell_0} \equiv 1 \bmod m. \tag{🗀}$$

One the other hand, let $c$ be the number of cycles in the dynamical system. Then, since $\#\underline{\mathsf{U}}(m) = \varphi(m)$, necessarily

$$\varphi(m) = c\ell_0. \tag{📂}$$

Therefore,

$$u^{\varphi(m)} \underset{(📂)}{=} (u^{\ell_0})^c \underset{(📁)}{\equiv} 1^c = 1 \bmod m$$

□

**Corollary 7.10** (Fermat's little theorem)**.** *Given a prime $p$, let $x$ be any integer such that $p \mid x$. Then*

$$x^{p-1} \equiv 1 \bmod p$$

*If we rewrite the above expression as $x^p \equiv x \bmod p$, this holds true even for $x$ divisible by $p$.*

*Proof.* Let $p$ and $x$ be as in the statement. We have that $[x]_p \in \underline{\mathsf{U}}(p)$. Since $\varphi(p) = p - 1$, Theorem 7.9 gives us

$$x^{p-1} \equiv [x]_p^{p-1} \equiv 1 \bmod p$$

Multiplying by $x$ gives us

$$x^p \equiv x \bmod p \tag{🔑}$$

If $p \mid x$, both sides of the congruence are $\equiv 0 \bmod p$. Therefore (🔑) holds for for all integers $x$. □

**Example 7.11.** Simplify $2^{2021} \bmod 9$

*Answer.* Note $\underline{\mathsf{U}}(9) = \{1, 2, 4, 5, 7, 8\}$; so $\varphi(9) = 6$ and therefore $2^6 \equiv 1 \bmod 9$ since $\gcd(2, 9) = 1$. Now, $2021 = 336 \cdot 6 + 5$; so

$$\begin{aligned} 2^{2021} = (2^6)^{336} \cdot 2^5 &\equiv 2^5 \bmod 9 \\ &\equiv 5 \bmod 9 \end{aligned}$$

On the other hand, $3^6 = 9^3 \equiv 0 \bmod 9 \not\equiv 1 \bmod 9$, since $\gcd(3, 9) \neq 1$. 👆

**Corollary 7.12.** *Let $m$ be a modulus and $u \in \underline{\mathsf{U}}(m)$. Then, for any integer $b, c$ such that $b \equiv c \bmod \varphi(m)$, we have*

$$u^b \equiv u^c \bmod m$$

## 7.4. Primality Testing

**Primality Testing** refers to attempts to answering the questions:

*given a number $N$, how do we determine whether $N$ is a prime?*

One way is to find the prime factorisation of $N$, this is usually hard.

A zero-knowledge approach is to see if there's an integer $0 < x < N$ such that $x \mid N$.

**Proposition 7.13.** *Let $N \geqslant 3$, and suppose no integer $1 < x \leqslant \sqrt{N}$ divides $N$. Then $N$ must be prime.*

*Proof.* We prove the contrapositive; suppose $N$ is composite. Then $N = ab$, where $1 < a, b < N$. Without loss of generality, let $a \leqslant b$, then

$$a^2 \leqslant ab = N$$

Therefore, $1 < a \leqslant \sqrt{N}$. Hence, we have found an $a$ such that $1 < a \leqslant \sqrt{N}$ and $a \mid N$. □

For example, if $N \sim 2^{2000}$, we only need to check for divisors $\leqslant \sqrt{N} \sim 2^{1000}$. This motivates **sieve methods**.

A consequence of Corollary 7.10 is: if, for some $1 < u < N$, we have $u^{N-1} \equiv 1 \bmod N$, then $N$ is not a prime.

The converse is *not* true.

**Definition 7.14.** A composite number $M$ is called a **Carmichael number** if, for every integer $a$ coprime to $M$,

$$a^{M-1} \equiv 1 \bmod M \quad \text{or, equivalently,} \quad a^M \equiv a \bmod M$$

The smallest Carmichael number is $M = 561$.

## Problems

**Problem 7.1.** Consider the following modular dynamical system, which is neither additive nor multiplicative.

(a) Let $X = \underline{\mathsf{R}}(13) = \{0, 1, 2, \ldots, 12\}$ and let $f : X \to X$ be given by

$$x \mapsto f(x) \coloneqq [x^2 + 3]_{13}.$$

Draw the complete diagram for the dynamics of $f$, accounting for every element of $X$.

(b) Let $z_0 = 0$ and let $z_{n+1} = f(z_n)$ for all integers $n \geqslant 0$. What is $z_{2026}$?

**Problem 7.2.**

(a) Compute the length of the cycles in the dynamics of $\mathbf{M}_u$ on $(\mathbb{Z}/8\mathbb{Z})^\times$ for every $u \in \underline{\mathsf{U}}(8)$. Compare the length with $\varphi(8)$.

(b) Compute the length of the cycles in the dynamics of $\mathbf{M}_3$ on $(\mathbb{Z}/14\mathbb{Z})^\times$. Compare the length with $\varphi(14)$.

**Problem 7.3.** For a modulus $m$ and an integer $u \in \underline{\mathsf{U}}(m)$. In Lemma 7.8 we saw the dynamics of $\mathbf{M}_u$ on $(\mathbb{Z}/m\mathbb{Z})^\times$ consists of cycles of all of the same length $\ell_u$. In particular, $\ell_u$ is the smallest positive integer such that

$$a^{\ell_u} \equiv 1 \bmod m$$

Prove that if there exists a positive integer $k$ such that $a^k \equiv 1 \bmod m$, then $\ell_u \mid k$.

Hint. Apply the division lemma to $k$ and $\ell_u$ and use the minimality of $\ell_u$ to conclude that the remainder must be 0.

**Problem 7.4.** A **Sophie Germain prime** is a prime number $p$ such that $2p+1$ is also a prime. For example, $p = 2, 3, 5$ are Sophie Germain primes, but $p = 7$ is not (since $15 = 2 \cdot 7 + 1$ is not a prime).

Prove that if $p$ is a Sophie Germain prime, then $2p + 1$ is either a divisor of $2^p - 1$ or of $2^p + 1$, but not of both.

**Problem 7.5.** Suppose that $p$ is a prime such that $p \equiv 2 \bmod 3$. Prove that every integer is a cube modulo $p$.

That is, prove that for every integer $x$ there exists an integer $a$ such that $x \equiv a^3 \bmod p$.

**Problem 7.6.** Consider the recursive sequence given by

$$a_0 = 3, \quad a_n = 3^{a_{n-1}}, \quad \text{for } n \geqslant 1$$

That is, $a_0 = 3,\ a_1 = 3^3,\ a_2 = 3^{3^3}, \ldots$. What is the last digit of $a_{1000}$?

**Problem 7.7.** Recall that a composite integer $M$ is a Carmichael number, if for every $a \in \mathbb{Z}$, we have

$$a^M \equiv a \bmod M$$

In this problem you will prove some composite numbers to be Carmichael numbers and prove some properties of Carmichael numbers.

(a) The number 561 factors as $3 \cdot 11 \cdot 17$. First use Fermat's little theorem to prove that

$$a^{561} \equiv a \bmod 3, \quad a^{561} \equiv a \bmod 11, \quad \text{and} \quad a^{561} \equiv a \bmod 17$$

for every value of $a$.

Then explain why these three congruences imply that $a^{561} \equiv a \bmod 561$ for every value of $a$.

Hint. Problem 1.7.

(b) Show that you can mimic the idea used in (a) to prove that each of the following numbers is a Carmichael number. (To assist you, we have factored each number into primes.)

(i) $1729 = 7 \cdot 13 \cdot 19$

(ii) $10585 = 5 \cdot 29 \cdot 73$

(iii) $75361 = 11 \cdot 13 \cdot 17 \cdot 31$

(iv) $1024651 = 19 \cdot 199 \cdot 271$

(c) Prove that a Carmichael number must be odd.

Hint. Assume $M$ is an even Carmichael number, what happens when $a = M - 1$.

(d) Prove that a Carmichael number must be square-free, i.e., it is a product of distinct primes.

Hint. Assume there is a prime $p$ such that $p^2 \mid M$, a Carmichael number. Then, argue that you have $a^{M-1} \equiv 1 \bmod p^2$ for integers $a$ such that $\gcd(a, M) = 1$. Argue that this means $\varphi(p^2) \mid (M - 1)$. Compute $\varphi(p^2)$ to conclude $p \mid (M - 1)$. Arrive at a contradiction.

(e) Look up **Korselt's criterion** in a book or online, write a brief description of how it works, and use it to show that $29341 = 13 \cdot 37 \cdot 61$ and $172947529 = 307 \cdot 613 \cdot 919$ are Carmichael numbers.

# 8. Arithmetic Functions II

## 8.1. Euler-Totient Function

**Theorem 8.1.** *Let $n$ be a positive integer with prime factorisation $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$. Then*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_t}\right)$$

*Proof.* Recall that

$$\varphi(n) = \#\underline{\mathsf{U}}(n) = \#\left\{i \in \mathbb{Z} \ : \ 0 \leqslant i < n, \ \gcd(i,n) = 1\right\}.$$

Consider the sets

$$\begin{aligned}
\underline{\mathsf{R}}(n) &= \{0, 1, \ldots, n-1\} \\
D_1 &= \left\{a \in \underline{\mathsf{R}}(n) \ : \ p_1 \mid a\right\} \\
D_2 &= \left\{a \in \underline{\mathsf{R}}(n) \ : \ p_2 \mid a\right\} \\
&\vdots \\
D_t &= \left\{a \in \underline{\mathsf{R}}(n) \ : \ p_t \mid a\right\}
\end{aligned}$$

Note that

$$\begin{aligned}
\underline{\mathsf{U}}(n) &= \left\{a \in \underline{\mathsf{R}}(n) \ : \ p_i \nmid a, \text{ for all } i = 1, \ldots, t\right\} \\
&= \left\{a \in \underline{\mathsf{R}}(n) \ : \ a \notin D_i, \text{ for all } i = 1, \ldots, t\right\} \\
&= \underline{\mathsf{R}}(n) \setminus \cup_{i=1}^{t} D_i,
\end{aligned}$$

So we need to compute

$$\#\left(\underline{\mathsf{R}}(n) \setminus \cup_{i=1}^{t} D_i\right) = \#\underline{\mathsf{R}}(n) - \#\left(\cup_{i=1}^{t} D_i\right) = n - \#\left(\cup_{i=1}^{t} D_i\right),$$

In particular, we must compute $\#\left(\cup_{i=1}^{t} D_i\right)$; which, by the inclusion–exclusion principle, is

$$\#\left(\bigcup_{i=1}^{t} D_i\right) = \left(\sum_{k=1}^{t} (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant t} \#\left(D_{i_1} \cap D_{i_2} \cap \cdots \cap D_{i_k}\right)\right)$$

> For any choice of indices $1 \leqslant i_1 < \cdots < i_k \leqslant t$ we claim
>
> $$\#\left(D_{i_1} \cap \cdots \cap D_{i_k}\right) = \frac{n}{p_{i_1} \cdots p_{i_k}}$$
>
> Since the primes $p_1, \ldots, p_t$ are distinct, we have
>
> $$\begin{aligned}
> D_{i_1} \cap \cdots \cap D_{i_k} &= \left\{a \in \underline{\mathsf{R}}(n) \ : \ p_{i_1} \mid a, \ldots, p_{i_k} \mid a\right\} \\
> &= \left\{a \in \underline{\mathsf{R}}(n) \ : \ p_{i_1} \cdots p_{i_k} \mid a\right\} \\
> &= \left\{a \in \underline{\mathsf{R}}(n) \ : \ a = p_{i_1} \cdots p_{i_k} b, \text{ for some } b \in \mathbb{Z}\right\} \\
> &= \left\{p_{i_1} \cdots p_{i_k} b \ : \ 0 \leqslant p_{i_1} \cdots p_{i_k} b < n\right\} \\
> &= \left\{p_{i_1} \cdots p_{i_k} b \ : \ 0 \leqslant b < \frac{n}{p_{i_1} \cdots p_{i_k}}\right\} = \frac{n}{p_{i_1} \cdots p_{i_k}}
> \end{aligned}$$
>
> as claimed. □

We return to our calculations,

$$\begin{aligned}
\varphi(n) &= \#\underline{\cup}(n) \\
&= n - \left( \sum_{k=1}^{t} (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant t} \#\left(D_{i_1} \cap D_{i_2} \cap \cdots \cap D_{i_k}\right) \right) \\
&= n - \left( \sum_{k=1}^{t} (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant t} \frac{n}{p_{i_1} \cdots p_{i_k}} \right) \\
&= n \left( 1 - \left( \frac{1}{p_1} + \cdots + \frac{1}{p_2} \right) + \left( \sum_{1 \leqslant i_1 < i_2 \leqslant t} \frac{1}{p_{i_1} p_{i_2}} \right) + \cdots + (-1)^t \frac{1}{p_1 \cdots p_t} \right) \\
&= n \left( 1 - \frac{1}{p_1} \right) \left( 1 - \frac{1}{p_2} \right) \cdots \left( 1 - \frac{1}{p_t} \right)
\end{aligned}$$

Hence $\varphi(n) = n \left( 1 - \frac{1}{p_1} \right) \left( 1 - \frac{1}{p_2} \right) \cdots \left( 1 - \frac{1}{p_t} \right)$.

**Corollary 8.2.** *Let $p$ be a prime, then $\varphi(p^e) = p^{e-1}(p-1)$ for any integer $e \geqslant 1$.*

**Corollary 8.3.** *$\varphi$ is multiplicative. That is, for positive integers $a, b$ such that $\gcd(a,b) = 1$, we have*

$$\varphi(ab) = \varphi(a)\varphi(b)$$

**Example 8.4** (in-class)**.** Compute $\varphi(72)$, and then compute (the natural representative of) $5^{2403} \bmod 72$.

## 8.2. Discrete Convolution

Recall from Problem 3.9 the **convolution** of two multiplicative functions $f, g : \mathbb{Z}_+ \to \mathbb{C}$,

$$(f * g) \colon \mathbb{Z}_+ \to \mathbb{C}, \quad (f * g)(n) \coloneqq \sum_{d \in \mathscr{D}(n)} f(d) g\left(\frac{n}{d}\right),$$

which is also multiplicative.

Consider $f = \mu$, the Möbius function (Problem 3.8) and $g = \mathrm{id}$, i.e., $g(n) = n$ for all positive integers $n$.

For a prime $p$ and integer $e \geqslant 0$, observe

$$\begin{aligned}
(\mu * \mathrm{id})(p^e) &= \sum_{d \in \mathscr{D}(p^e)} \mu(d)\, \mathrm{id}\left(\frac{n}{d}\right) \\
&= \sum_{k=0}^{e} \mu(p^k) \left( \frac{p^e}{p^k} \right) \\
&= \mu(1)p^e + \mu(p)p^{e-1} + \sum_{k=2}^{e} \mu(p^k) p^{e-k} \\
&= p^e - p^{e-1} && \text{since } \mu(p^k) = 0, \text{ for } k \geqslant 2 \\
&= p^{e-1}(p-1) \\
&= \varphi(p^e)
\end{aligned}$$

Hence, by multiplicativity of $\mu * \mathrm{id}$ and $\varphi$, we conclude that

$$\mu * \mathrm{id} = \varphi$$

**Lemma 8.5.** *Let $n$ be a positive integer, then we have*

$$\sum_{d \in \mathscr{D}(n)} \varphi(d) = n$$

*Proof.* We have $\varphi = \mu * \mathrm{id} = \mathrm{id} * \mu$, by computations above and Problem 8.2 below.

From Problem 3.8 we know that

$$\sum_{d \in \mathscr{D}(n)} \mu(d) = \varepsilon(n) \coloneqq \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases} \tag{☕}$$

Let $\mathbb{1} : \mathbb{Z}_+ \to \mathbb{C}$ be the constant function that's identically 1, i.e., $\mathbb{1}(n) = 1$ for every $n$.

Then (☕) can be rewritten as follows

$$(\mu * \mathbb{1})(n) = \sum_{d \in \mathscr{D}(n)} \mu(d)\, \mathbb{1}\left(\frac{n}{d}\right) = \sum_{d \in \mathscr{D}(n)} \mu(d) \cdot 1 = \sum_{d \in \mathscr{D}(n)} \mu(d) = \varepsilon(n)$$

That is, we have $\mu * \mathrm{id} = \varepsilon$. We may similarly observe that

$$\sum_{d \in \mathscr{D}(n)} \varphi(d) = (\varphi * \mathbb{1})(n)$$

Now, using Problem 8.2, we get

$$\begin{aligned} \varphi * \mathbb{1} &= (\mathrm{id} * \mu) * \mathbb{1} \\ &= \mathrm{id} * (\mu * \mathbb{1}) \\ &= \mathrm{id} * \varepsilon \\ &= \mathrm{id} \end{aligned}$$

Therefore,

$$\sum_{d \in \mathscr{D}(n)} \varphi(d) = (\varphi * \mathbb{1})(n) = \mathrm{id}(n) = n. \qquad \square$$

## Problems

**Problem 8.1.** Prove that $\varphi(n)$ is even for any integer $n > 2$.

**Problem 8.2.** Let $f(n)$ and $g(n)$ be two complex-valued functions of positive integers $n > 0$, not necessarily multiplicative. Recall the definition of convolution

$$(f * g)(n) = \sum_{d \in \mathscr{D}(n)} f(d) g\left(\frac{n}{d}\right) = \sum_{\substack{ab=n \\ a,b>0}} f(a) g(b).$$

(a) Prove that the two functions $f * g$ and $g * f$ are one and the same.
(In other words: the convolution product is commutative.)

(b) Let $\varepsilon(n)$ be the function defined by the rule

$$\varepsilon(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}.$$

Prove that $f = \varepsilon * f$. Combined with (a), this tell us $f * \varepsilon = f = \varepsilon * f$.
(In other words: $\varepsilon$ acts as the neutral element for the convolution.)

(c) Let $h : \mathbb{Z}_+ \to \mathbb{C}$ be a third arithmetic function. Prove that

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

(In other words, the convolution product is associative.)

(d) Suppose that $f(1) \neq 0$. Define the function $i_f(n)$ by induction on the divisibility of $n$ as follows. First define

$$i_f(1) \coloneqq \frac{1}{f(1)}. \tag{✋}$$

Given an integer $n > 1$, assume we have defined $i_f(d)$ for all the proper positive divisors $d$ of $n$. Define

$$i_f(n) \coloneqq -\frac{1}{f(1)} \sum_{\substack{d \in \mathscr{D}(n) \\ d<n}} i_f(d) f\left(\frac{n}{d}\right). \tag{✋}$$

Let $f = \mathrm{id}$. Compute $i_f(n)$ for $n = 2, 3, 4, 5, 6$.

(e) Suppose $f : \mathbb{Z}_+ \to \mathbb{C}$ is any arithmetic function with $f(1) \neq 0$, and $i_f$ is as defined (inductively) in (d). Prove that $i_f * f = \varepsilon$.

(f) For $f$ as in (e), prove that if $j : \mathbb{Z}_+ \to \mathbb{C}$ is any other arithmetic function such that $j * f = \varepsilon$, then $j = i_f$.
Hint: look back to our proof of "uniqueness" of multiplicative inverses modulo $m$.

**Problem 8.3** (Möbius Inversion)**.** Let $f, g : \mathbb{Z}_+ \to \mathbb{C}$ be two arithmetic functions. Prove that

$$g(n) = \sum_{d \in \mathscr{D}(n)} f(d) \quad \text{if and only if} \quad f(n) = \sum_{d \in \mathscr{D}(n)} \mu(d) g\left(\frac{n}{d}\right)$$

Equivalently, in the language of convolution, prove that $g = f * \mathbb{1}$ if and only if $f = g * \mu$.

This is called the **Möbius Inversion formula**. Our proof of Lemma 8.5 secretly used this.

**Problem 8.4.** For any integer $k \geqslant 0$, define $p_k : \mathbb{Z}_+ \to \mathbb{C}$ as $p_k(n) = n^k$. In particular, $p_0 = \mathbb{1}$ and $p_1 = \mathrm{id}$. Prove that

$$p_k = \sigma_k * \mu,$$

using Möbius inversion.

**Problem 8.5.** The **von Mangoldt function** is an arithmetic function, important due to its relation to the Riemann zeta function, which is neither multiplicative not additive. It is defined as

$$\Lambda(n) = \begin{cases} \ln(p) & \text{if } n = p^e \text{ for some prime } p \text{ and integer } e \geqslant 1 \\ 0 & \text{otherwise} \end{cases}$$

(a) Prove that

$$\sum_{d \in \mathscr{D}(n)} \Lambda(d) = \ln(n)$$

(b) Using Möbius inversion, prove that

$$\Lambda(n) = -\sum_{d \in \mathscr{D}(n)} \mu(d) \ln(d)$$

**Remark 8.6.** You may have heard about the **Riemann zeta function**. As an arithmetic function

$$\zeta : \mathbb{Z}_+ \to \mathbb{C}, \ \zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$$

it has the following relation to the Möbius function as an application of Möbius inversion

$$\frac{1}{\zeta(k)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^k}$$

The logarithmic derivative of the Riemann zeta function is

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

where $\Lambda$ is the von Mangoldt function defined in the previous problem.

# 9. Primitive Roots & Polynomials Modulo $p$

Fix $p$ a prime. We let $\mathbb{F}_p \coloneqq \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$. Furthermore, $\mathbb{F}_p^\times \coloneqq (\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{1}, \ldots, \overline{p-1}\}$.

## 9.1. Primitive Roots Modulo $p$

For $u \in \underline{\mathsf{U}}(p)$, equivalently $p \nmid u$, we define $\ell(u)$ as the length of the cycles in the dynamics of $\mathbf{M}_u$ on $\mathbb{F}_p^\times$.

We have seen, while proving Theorem 7.9 (Euler-Fermat Theorem), that $\ell(u) \mid \varphi(p) = p-1$.

**Definition 9.1.** Say $u$ is a **primitive root modulo $p$** if $\ell(u) = p-1$.

Equivalently, if there's exactly one cycle in the dynamics of $\mathbf{M}_u$ on $\mathbb{F}_p^\times$.

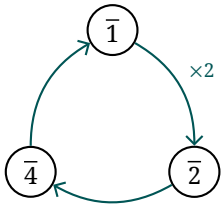
For example, for $p = 7$, consider

$u = 1$



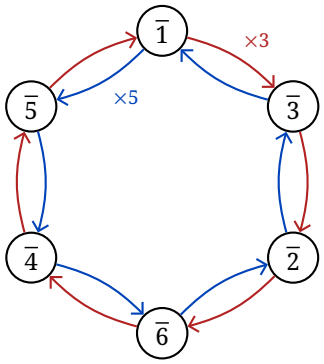

$\ell(1) = 1 \neq 7-1$, so 1 is *not* primitive.

$u = 2$




$\ell(2) = 3 \neq 7-1$, so 2 is *not* primitive.

$u = 3$




$\ell(3) = 6 = 7-1$, so 3 *is primitive*.

So is 5, as the multiplicative inverse of 3 modulo 7 in $\mathbb{F}_7^\times$.

The main theorem we will prove in this section is:

**Theorem** (Primitive Root Theorem; Gauss)**.** *There exist $\varphi(p-1)$-many primitive roots in $\mathbb{F}_p^\times$.*

**Example 9.2.** For $p = 7$, note that $\varphi(7-1) = \varphi(6) = \varphi(2)\varphi(3) = 1 \cdot 2 = 2$. The theorem tells us that there are 2 primitive roots modulo 7, they are necessarily 3 and 5, as seen in the example above.

## 9.2. Polynomials Modulo $p$

**Definition 9.3.** Let $p$ be a prime number, a polynomial modulo $p$ is an expression

$$f(T) = a_d T^d + \cdots + a_1 T + a_0$$

where the coefficients $a_0, \ldots, a_d \in \mathbb{F}_p$. The set of all polynomials modulo $p$ is denoted $\mathbb{F}_p[T]$.

The **degree** of $f(T)$, denoted $\deg f$, is the largest $d$ such that $a_d \neq \overline{0}$ in $\mathbb{F}_p$.

We also adopt the convention that $\deg 0 := -\infty$, where 0 is the zero polynomial.

We can add, subtract and multiply polynomials modulo $p$, similar to regular polynomials.

For example, let $p = 5$. Consider the following polynomials in $\mathbb{F}_5[T]$

$$f(T) = \overline{4}T + \overline{2} \quad \text{and} \quad g(T) = \overline{3}T^2 + \overline{2}T$$

Then $\deg f = 1$ and $\deg g = 2$. Moreover, we have

$$\begin{aligned} f(T) + g(T) &= (\overline{4}T + \overline{2}) + (\overline{3}T^2 + \overline{2}T) \\ &= \overline{3}T^2 + \overline{6}T + \overline{2} \\ &= \overline{3}T^2 + T + \overline{2} && \text{reducing mod 5} \end{aligned}$$

$$\begin{aligned} f(T)g(T) &= (\overline{4}T + \overline{2}) \cdot (\overline{3}T^2 + \overline{2}T) \\ &= \overline{12}T^3 + \overline{6}T^2 + \overline{8}T^2 + \overline{4}T \\ &= \overline{12}T^3 + \overline{14}T^2 + \overline{4}T \\ &= \overline{2}T^3 + \overline{4}T^2 + \overline{4}T && \text{reducing mod 5} \\ &= \overline{2}T^3 - T^2 - T && \text{manipulating coefficients mod 5} \end{aligned}$$

**Lemma 9.4.** *Let $p$ be a prime, and consider $a, b \in \mathbb{F}_p$ such that $a, b \neq \overline{0}$. Then $ab \neq \overline{0}$.*

*Proof.* For $a, b \in \mathbb{F}_p$, we may write $a = \overline{x}$ and $b = \overline{y}$ for integers $a, b$. Since $a, b \neq \overline{0}$, this is equivalent to

$$x, y \not\equiv 0 \bmod p, \quad \text{equivalently} \quad p \nmid x \text{ and } p \nmid y$$

Applying the contrapositive of Corollary 2.4, we obtain $p \nmid xy$. This is equivalent to $xy \not\equiv 0 \bmod p$, allowing us to conclude $ab = \overline{xy} \neq \overline{0}$. □

**Theorem 9.5.** *Let $p$ be a prime and $f(T)$, $g(T) \in \mathbb{F}_p[T]$ are non-zero. Then*

$$\deg(fg) = \deg f + \deg g$$

*Proof.* Let $d = \deg f$ and $e = \deg g$, then

$$f(T) = a_d T^d + (\text{lower order terms}), \quad a_d \neq \overline{0}$$

$$g(T) = b_e T^e + (\text{lower order terms}), \quad b_e \neq \overline{0}$$

Then

$$f(T)g(T) = a_d b_e T^{d+e} + (\text{lower order terms}).$$

Since $a_d, b_e \neq \overline{0}$, by Lemma 9.4 we obtain $a_d b_e \neq \overline{0}$. Therefore $\deg(fg) = d + e = \deg f + \deg g$. □

**Remark 9.6.** For a composite modulus $m$, we can similarly consider polynomials modulo $m$ which we can add, subtract and multiply such polynomials. But Theorem 9.5 above does not hold for these polynomials.

For example, let $m = 6$, and consider the following polynomials modulo 6

$$f(T) = \overline{3}T + \overline{2}, \qquad g(T) = \overline{2}T^3$$

So,

$$f(T)g(T) = \overline{6}T^4 + \overline{4}T^3 = \overline{0}T^4 + \overline{4}T^3 = \overline{4}T^3.$$

Then $\deg(fg) = 3 \neq 4 = \deg f + \deg g$.

**Definition 9.7.** An element $a$ of $\mathbb{F}_p$ is a **root** of $f(T) \in \mathbb{F}_p[T]$, if $f(a) = \overline{0}$.

Say an integer $x$ is a root of a polynomial modulo $p$ if $\overline{x}$ is.

For example, consider $p = 5$ the polynomial $g(T) = \overline{3}T^2 + \overline{2}T$ modulo 5.

- $x = 0$ is a root of $g(T)$, since $g(\overline{0}) = \overline{0}$.
- $x = 1$ is a root of $g(T)$, since $g(\overline{1}) = \overline{3} \cdot \overline{1}^2 + \overline{2} \cdot \overline{1} = \overline{5} = \overline{0}$.
- $x = 2$ is *not* a root of $g(T)$, since $g(\overline{2}) = \overline{3} \cdot \overline{2}^2 + \overline{2} \cdot \overline{2} = \overline{16} = \overline{1} \neq \overline{0}$.

**Proposition 9.8.** *A linear polynomial $f(T) = aT + b \in \mathbb{F}_p[T]$ has a unique root in $\mathbb{F}_p$.*

*Proof.* Since $f(T) = aT + b$ is a linear polynomial, necessarily $a \neq \overline{0}$. Therefore, there exists a unique $c \in \mathbb{F}_p$ such that $ac = \overline{1}$, by Corollary 6.16. Consider an $x \in \mathbb{Z}$, then $x$ is a root of $f(T)$ if and only if $f(\overline{x}) = a\overline{x} + b = 0$ if and only if $a\overline{x} = -b$ if and only if $\overline{x} = -cb$. □

$\mathbb{F}_p[T]$, the set of polynomials modulo $p$, behaves a lot like $\mathbb{Z}$.

**Theorem 9.9** (Division Lemma for mod-$p$ Polynomials)**.** *Let $p$ be a prime, and consider $f(T)$, $g(T) \in \mathbb{F}_p[T]$. Assume $g(T)$ is not the zero polynomial (*$\deg g \geqslant 0$*). Then there exist unique polynomials $q(T)$ and $r(T)$ modulo $p$ such that*

$$f(T) = g(T)q(T) + r(T), \quad 0 \leqslant \deg r < \deg g$$

*That is, we can perform long division in $\mathbb{F}_p[T]$.*

For example, consider $p = 5$ and polynomials $f(T) = T^3 + \overline{4}T + \overline{2}$ and $g(T) = T^2 + T + \overline{2}$ modulo 5.

Let us perform long division!

$$\begin{array}{rl} & T - \overline{1} \\ T^2 + T + \overline{2} \,\overline{)\, T^3 + \overline{0}T^2 + \overline{4}T + \overline{2}} & \\ \underline{T^3 + \ T^2 + \overline{2}T} & \text{(subtract)} \\ -\ T^2 + \overline{2}T + \overline{2} & \\ \underline{-\ T^2 - \ T - \overline{2}} & \text{(subtract)} \\ \overline{3}T + \overline{4} & \end{array}$$

Therefore

$$f(T) = \underbrace{(T - \overline{1})}_{q(T)} g(T) + \underbrace{(\overline{3}T + \overline{4})}_{r(T)}$$

**Definition 9.10.** Let $p$ be a prime number, and "a polynomial" below refers to polynomials modulo $p$

- A **unit polynomial** is a non-zero constant polynomial; a polynomial of degree 0. That is, it of the form
$$u(T) = a \neq \overline{0}$$
- A polynomial $f(T)$ is an **irreducible polynomial** if
  (I1) $\deg f \geqslant 1$, i.e., it is a non-constant polynomial; and
  (I2) If $g(T)$ and $h(T)$ are polynomials such that
  $$f(T) = g(T)h(T)$$
  then either $g(T)$ is a unit polynomial, or $h(T)$ is.

*Informally, an irreducible polynomial is one that cannot be factored into non-constant polynomials of lower degree.*

We have the following analogy with $\mathbb{Z}$

$$\text{unit polynomials} \longleftrightarrow \pm 1 \text{ in } \mathbb{Z}$$

$$\text{irreducible polynomials} \longleftrightarrow \text{prime numbers in } \mathbb{Z}$$

**Example 9.11.** For any $a \in \mathbb{F}_p$, the linear polynomial $f(T) = T - a \in \mathbb{F}_p[T]$ is irreducible.

*Answer.* Clearly (I1) of Definition 9.10 is met. Let us prove (I2); suppose

$$T - a = g(T)h(T).$$

Since $T - a$ is not the zero polynomial, necessarily $\deg g, \deg h \geqslant 0$. Now,

$$1 = \deg(T - a) = \deg g + \deg h.$$

Therefore, $\deg g = 0$ and $\deg h = 1$, or vice versa. Hence $g(T)$ is a unit, or $h(T)$ is. Thus, $f(T)$ is irreducible. □

In fact, there are infinitely many irreducible polynomials modulo $p$. One proves this similarly as one proves the infinitude of primes once one has Theorem 9.13.

**Definition 9.12.** Let $p$ be a prime and $f(T) \in \mathbb{F}_p[T]$. Let $d = \deg f$, and write

$$f(T) = a_d T^d + \cdots + a_1 T + a_0; \quad \text{necessarily } a_d \neq \overline{0}.$$

We call $a_d$ the **leading coefficient of $f(T)$**. If $a_d = \overline{1}$, call $f(T)$ a **monic polynomial**.

Any non-zero polynomial $f(T)$ with leading coefficient $a_d$ can be uniquely written as

$$f(T) = a_d \cdot (\text{monic polynomial})$$

**Theorem 9.13** (Unique factorisation of mod-$p$ Polynomials)**.** *Let $f(T)$ be a non-zero polynomials modulo $p$, where $p$ is prime. Then $f(T)$ can be uniquely written as*

$$f(T) = c \cdot h_1(T)^{e_1} h_2(T)^{e_2} \cdots h_r(T)^{e_r}$$

*where*

(a) *$c$ is the leading coefficient of $f(T)$;*

(b) *$h_1(T), h_2(T), \ldots, h_r(T)$ are monic irreducible polynomials modulo $p$; and*

(c) *$e_1, \ldots, e_r > 0$ are integers.*

*Proof.* The proof is similar to the proof of uniqueness of prime factorisation in $\mathbb{Z}$, Theorem 2.5. One applies (strong) induction on $\deg f$. □

**Lemma 9.14.** *Let $p$ be prime, and $f(T) \in \mathbb{F}_p[T]$ with $x \in \mathbb{Z}$. Then $x$ is a root of $f(T)$ if and only if $T - \overline{x}$ divides $f(T)$.*

*Proof.* We apply the division lemma to $f(T)$ and $T - \overline{x}$: there exist $q(T), r(T) \in \mathbb{F}_p[T]$ such that

$$f(T) = (T - \overline{x}) \cdot q(T) + r(T), \quad \text{where } \deg r < \deg(T - \overline{x}) = 1.$$

Therefore $\deg r = 0$ or $-\infty$, i.e., $r(T)$ is a constant polynomial. Say, $r = r(T) \in \mathbb{F}_p$; so we have

$$f(T) = (T - \overline{x}) \cdot q(T) + r$$

$x$ is a root of $f(T)$ if and only if $f(\overline{x}) = 0$ if and only if

$$0 = f(\overline{x}) = (\overline{x} - \overline{x}) \cdot q(\overline{x}) + r = r \quad \text{, equivalently, if and only if } r = 0.$$

Hence $f(T)$ has $\overline{x}$ as a root if and only if $f(T) = (T - \overline{x}) \cdot q(T)$ if and only if $T - \overline{x}$ divides $f(T)$. □

**Example 9.15.** Consider $f(T) = T^3 + \overline{2} \in \mathbb{F}_5[T]$. Let us find the unique factorisation into irreducibles of $f$.

*Answer.* First, we check if $f(T) = T^3 + \overline{2}$ has a root modulo 5; note

| $a$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
|---|---|---|---|---|---|
| $f(a) = a^3 + \overline{2}$ | $\overline{0} + \overline{2} = \overline{2}$ | $\overline{1} + \overline{2} = \overline{3}$ | $\overline{8} + \overline{2} = \overline{0}$ | $\overline{27} + \overline{2} = \overline{4}$ | $\overline{64} + \overline{2} = \overline{1}$ |

Therefore $\overline{2}$ is a root of $f(T)$, hence by Lemma 9.14 we have that $T - \overline{2}$ divides $f(T)$. Thus,

$$f(T) = (T - \overline{2}) \cdot g(T),$$

for some polynomial $g(T) \in \mathbb{F}_5[T]$ and $\deg g = 2$. We employ long division to compute $g(T)$

$$\begin{array}{rl} & T^2 + \overline{2}T + \overline{4} \\ T - \overline{2} \,\big)\, & T^3 + \overline{0}T^2 + \overline{0}T + \overline{2} \\ & \underline{T^3 - \overline{2}T^2} \qquad\qquad \text{(subtract)} \\ & \quad \overline{2}T^2 + \overline{0}T + \overline{2} \\ & \quad \underline{\overline{2}T^2 - \overline{4}T} \qquad\qquad \text{(subtract)} \\ & \qquad \overline{4}T + \overline{2} \\ & \qquad \underline{\overline{4}T - \overline{8}} \qquad\qquad \text{(subtract)} \\ & \qquad\quad \overline{10} = \overline{0} \end{array}$$

Therefore $g(T) = T^2 + \overline{2}T + \overline{4}$, hence

$$f(T) = (T - \overline{2})(T^2 + \overline{2}T + \overline{4}) = (T + \overline{3})(T^2 + \overline{2}T + \overline{4}) \qquad (\text{Y})$$

We are not done yet, since we should verify if $g(T) = T^2 + \overline{2}T + \overline{4}$ is irreducible, as $T + \overline{3}$ already is.

| $a$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
|---|---|---|---|---|---|
| $g(a) = a^2 + \overline{2}a + \overline{4}$ | $\overline{4}$ | $\overline{7} = \overline{2}$ | $\overline{12} = \overline{2}$ | $\overline{19} = \overline{4}$ | $\overline{28} = \overline{3}$ |

Thus, by Problem **??**, $g(T)$ is irreducible since it has no roots modulo 5.

Therefore the factorisation ($\text{Y}$) is the unique factorisation of $f$ into irreducibles. ☝

**Theorem 9.16.** *Let $p$ be a prime number and $f(T) \in \mathbb{F}_p[T]$. Assume that $f(T)$ is non-zero, then*

$$\#\{\textit{distinct roots of } f(T)\} \leqslant \deg f.$$

*Proof.* We will induct on $\deg f$. We consider two base cases: $\deg f = 0$ and 1.

Assume $\deg f = 0$, then $f(T) = c \in \mathbb{F}_p \setminus \{0\}$. Then, for no $a \in \mathbb{F}_p$, do we have $f(a) = \overline{0}$. Therefore

$$\#\{\text{distinct roots of } f(T)\} = 0 = \deg f.$$

Assume $\deg f = 1$, then $f(T) = aT + b$ with $a \neq \overline{0}$. By Proposition 9.8, $f$ has a unique root in $\mathbb{F}_p$. Therefore

$$\#\{\text{distinct roots of } f(T)\} = 1 = \deg f.$$

Assume the inductive hypothesis holds.

Assume $f(T)$ has no roots in $\mathbb{F}_p$, then the result holds since

$$\#\{\text{distinct roots of } f(T)\} = 0 \leqslant \deg f.$$

Assume now $f$ has a root, say $a \in \mathbb{F}_p$. Then, by Lemma 9.14, we have $f(T) = (T - a) \cdot g(T)$, for some polynomial $g(T) \in \mathbb{F}_p[T]$. Therefore, $\deg g = \deg f - 1$, by Theorem 9.5.

Hence, by the inductive hypothesis, $g(T)$ has at most $(\deg g)$-many distinct roots. Note,

$$\{\text{roots of } f(T)\} = \{a\} \cup \{\text{roots of } g(T)\}$$

Therefore,

$$\begin{aligned} \#\{\text{roots of } f(T)\} &\leqslant \#\{a\} + \#\{\text{roots of } g(T)\} \\ &\leqslant 1 + \deg g \\ &= 1 + (\deg f - 1) \\ &= \deg f \end{aligned}$$

Hence, the result holds, by the principle of mathematical induction. □

**Remark 9.17.** As in Remark 9.6, the assumption that $p$ is prime is important. As mentioned, for a composite modulus $m$, we can also consider polynomials modulo $m$ and define the notion of degree and roots of such polynomials.

But unlike in the case of primes, the number of roots of these polynomials are then not bounded by degree.

For example, let $m = 8$, and consider the polynomial $f(T) = T^2 - \overline{1}$ modulo 8. Note that

$$f(\overline{1}) = \overline{1}^2 - \overline{1} = \overline{0}$$

$$f(\overline{3}) = \overline{3}^2 - \overline{1} = \overline{8} = \overline{0}$$

$$f(\overline{5}) = \overline{5}^2 - \overline{1} = \overline{24} = \overline{0}$$

$$f(\overline{7}) = \overline{7}^2 - \overline{1} = \overline{48} = \overline{0}$$

It is clear that $\overline{1}$, $\overline{3}$, $\overline{5}$ and $\overline{7}$ are distinct elements in $\mathbb{Z}/8\mathbb{Z}$.

Therefore, we have found at least 4 roots of a degree 2 polynomial!

## 9.3. Proof of Primitive Root Theorem

**Definition 9.18** (Recall)**.** Let $p$ be a prime number and $u \in \underline{\mathsf{U}}(p)$, then

- $\ell(u)$ = the common length of the cycles in the dynamics of $\mathbf{M}_u$ on $\mathbb{F}_p^\times$

  = the smallest positive integer $\ell$ such that $a^\ell \equiv 1 \bmod p$
- $c(u)$ = the number of cycles in the dynamics of $\mathbf{M}_u$ on $\mathbb{F}_p^\times$

In the course of proving Theorem 7.9, we noted that $c(a) \cdot \ell(a) = \varphi(p) = \#\underline{\mathsf{U}}(p) = p - 1$.

**Lemma 9.19.** *Let $p$ be a prime and $\lambda > 0$ be an integer; define*

$$\underline{\mathsf{U}}(p;\lambda) \coloneqq \left\{u \in \underline{\mathsf{U}}(p) \ : \ \ell(u) = \lambda\right\}$$

*Then, the set $\underline{\mathsf{U}}(p;\lambda)$ is either empty or has $\varphi(\lambda)$-many elements. Necessarily $\lambda \mid (p-1)$.*

*Proof.* Assume $\underline{\mathsf{U}}(p;\lambda)$ is non-empty, we aim to prove that $\#\underline{\mathsf{U}}(p;\lambda) = \varphi(\lambda)$.

Consider $u \in \underline{\mathsf{U}}(p;\lambda)$; therefore $\ell(u) = \lambda$. For $e = 0, 1, \ldots, \lambda - 1$, we have

$$(u^e)^\lambda = (u^\lambda)^e \equiv 1^e \equiv 1 \bmod p$$

Hence, the polynomial $f(T) = T^\lambda - \overline{1} \in \mathbb{F}_p[T]$ has $u^0, u^1, \ldots, u^{\lambda-1}$ as roots.

Moreover, since $\ell(a) = \lambda$, these are necessarily distinct modulo $p$.

Since $\deg f = \lambda$ and we found $\lambda$-many distinct roots of $f$, the set of roots of $f$ is $\{u^e \ : \ 0 \leqslant e < \lambda\}$. Thus

$$T^\lambda - \overline{1} = (T - \overline{u}^0)(T - \overline{u}^1) \cdots (T - \overline{u}^{\lambda-1})$$

Consider an arbitrary $a \in \underline{\mathsf{U}}(p;\lambda)$; by assumption $\ell(a) = \lambda$ and so $a^\lambda \equiv 1 \bmod p$. Hence, $a$ is a root of $T^\lambda - \overline{1}$. Therefore, necessarily, $\overline{a} = \overline{u}^e$, for some $0 \leqslant e \leqslant \lambda - 1$.

Therefore every element of $\underline{\mathsf{U}}(p;\lambda)$ is $\equiv u^e \bmod p$ for some $1 \leqslant e \leqslant \lambda - 1$. We have obtained

$$\underline{\mathsf{U}}(p;\lambda) = \left\{[u^e]_p \ : \ 0 \leqslant e < \lambda \text{ and } \ell(u^e) = \lambda\right\}$$

Let us determine for which $e$ do we have $\ell(u^e) = \lambda$. If $k > 0$ is an integer such that $(u^e)^k \equiv 1 \bmod p$, then

$$u^{ek} \equiv 1 \bmod p \Leftrightarrow \ell(a) \mid ek \Leftrightarrow \lambda \mid ek \Leftrightarrow \frac{\lambda}{\gcd(e,\lambda)} \mid k$$

The first equivalence is Problem 7.3 and the last equivalence we justify below:

> Let $d = \gcd(e,\lambda)$. We wish to show that $\lambda \mid ek$ if and only if $(\lambda/d) \mid k$.
>
> ($\Rightarrow$) By Bézout's Identity $d = ex + \lambda y$ for some integers $x, y$. Therefore $dk = ekx + \lambda k y$. Since $\lambda \mid ek$ and clearly $\lambda \mid \lambda k$, hence $\lambda \mid (ekx + \lambda k y) = dk$ and thus $(\lambda/d) \mid k$.
>
> ($\Leftarrow$) Since $d \mid e$, hence $dk \mid ek$. By assumption $(\lambda/d) \mid k$, thus $\lambda \mid dk$. We conclude $\lambda \mid ek$ by Problem 1.2 (iii).

That is, any such $k$ is a multiple of $\lambda/\gcd(e,\lambda)$. Since $\ell(u^e)$ is the minimum such $k$, necessarily $\ell(u^e) = \lambda/\gcd(e,\lambda)$.

Hence, $\ell(u^e) = \lambda$ if and only if $\gcd(e,\lambda) = 1$. Thus,

$$\begin{aligned}
\#\underline{\mathsf{U}}(p;\lambda) &= \#\left\{[u^e]_p \ : \ 0 \leqslant e < \lambda \text{ and } \gcd(e,\lambda) = 1\right\} \\
&= \#\{e \ : \ 0 \leqslant e < \lambda \text{ and } \gcd(e,\lambda) = 1\} \\
&= \#\underline{\mathsf{U}}(\lambda) \\
&= \varphi(\lambda)
\end{aligned}$$

as claimed. □

**Theorem 9.20** (Primitive Root Theorem; Gauss)**.** *Let $p$ be prime. For $\lambda \mid (p-1)$, the set*

$$\underline{\mathsf{U}}(p;\lambda) \coloneqq \left\{u \in \underline{\mathsf{U}}(p) \ : \ \ell(u) = \lambda\right\} \neq \varnothing$$

*In particular, $\underline{\mathsf{U}}(p; p-1)$, the set of primitive roots modulo $p$, is non-empty and has exactly $\varphi(p-1)$-many elements.*

*Proof.* For any $u \in \underline{\mathsf{U}}(p)$, recall that $\ell(u) > 0$ and $\ell(u) \mid (p-1)$. Therefore $\ell(u) \in \mathscr{D}(p-1)$.

Now, for each $\lambda \in \mathscr{D}(p-1)$, Lemma 9.19 tells us that

$$\#\underline{\mathsf{U}}(p;\lambda) = \left\{u \in \underline{\mathsf{U}}(p) \ : \ \ell(u) = \lambda\right\} = 0 \text{ or } \varphi(\lambda)$$

Our aim is to prove that $\underline{\mathsf{U}}(p;\lambda) \neq \varnothing$. Note for $\lambda_1 \neq \lambda_2$, necessarily $\underline{\mathsf{U}}(p;\lambda_1) \cap \underline{\mathsf{U}}(p;\lambda_2) = \varnothing$. Therefore,

$$\underline{\mathsf{U}}(p) = \coprod_{\lambda \in \mathscr{D}(p-1)} \underline{\mathsf{U}}(p;\lambda)$$

Hence,

$$p - 1 = \#\underline{\mathsf{U}}(p) = \sum_{\lambda \in \mathscr{D}(p-1)} \#\underline{\mathsf{U}}(p;\lambda) \leqslant \sum_{\lambda \in \mathscr{D}(p-1)} \varphi(\lambda)$$

By Lemma 8.5, we also have that

$$\sum_{\lambda \in \mathscr{D}(p-1)} \varphi(\lambda) = p - 1$$

Suppose, there existed a $\lambda_0 \in \mathscr{D}(p-1)$ such that $\underline{\mathsf{U}}(p; \lambda_0) = \varnothing$, so $\#\underline{\mathsf{U}}(p; \lambda_0) = 0$. Then

$$\sum_{\lambda \in \mathscr{D}(p-1)} \varphi(\lambda) = p - 1 = \#\underline{\mathsf{U}}(p) = \sum_{\lambda \in \mathscr{D}(p-1)} \#\underline{\mathsf{U}}(p; \lambda) = \sum_{\lambda \in \mathscr{D}(p-1)\setminus\{\lambda_0\}} \#\underline{\mathsf{U}}(p; \lambda) \leqslant \sum_{\lambda \in \mathscr{D}(p-1)\setminus\{\lambda_0\}} \varphi(\lambda) < \sum_{\lambda \in \mathscr{D}(p-1)} \varphi(\lambda);$$

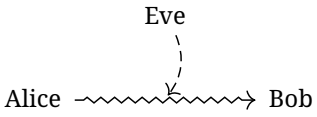
giving us a contradiction.

Thus, $\underline{\mathsf{U}}(p; \lambda) \neq \varnothing$, for all $\lambda \in \mathscr{D}(p-1)$. In particular, $\underline{\mathsf{U}}(p; p-1) \neq \varnothing$, and therefore

$$\#\underline{\mathsf{U}}(p; p-1) = \varphi(p-1). \qquad \square$$

## 9.4. Cryptographic Application: Diffie-Helman Key Exchange

Cryptography, *public* key system. Diffie-Helman key exchange.

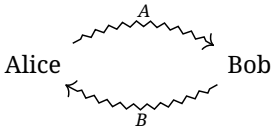



Alice wants to encrypt a message so that *only* Bob can decrypt it, not Eve.

(1) Alice chooses a prime $p$ ($\sim 2^{2000}$) such that $\varphi(p-1)$ also has a large prime factor, and finds a primitive root $g$ modulo $p$. Publishes $(p, g)$, the *public key*.

(2) Alice chooses $a \bmod p-1$ (*private key*) and computes $A \coloneqq g^a \bmod p$ and send it to Bob.

Bob chooses $b \bmod p-1$ (*private key*) and computes $B \coloneqq g^b \bmod p$ and sends it to Alice.




(3) Alice computes $B^a \bmod p$ and Bob computes $A^b \bmod p$, both are $\equiv g^{ab} \bmod p$. This is their secret $S$.

(4) Eve knows $(g, p, A, B)$. Can Eve find out what $S$ is?

This is very hard (that is, takes a lot of time and computation power). If Eve knows $a$ or $b$, then the security has been broken. But finding $a$ from $A \equiv g^a \bmod p$ is difficult. This is the *discrete logarithm problem*.

### Problems

**Problem 9.1.**

(a) Compute $\ell(u)$ in the $3 \times 4$ cases: $u = 2, 3, 6$ and $p = 7, 11, 13, 17$.

(b) For the primes $p = 7, 11, 13, 17$, list all the primitive roots modulo $p$.

**Problem 9.2.** Let $p$ be an odd prime and $\gamma$ a primitive root modulo $p$. That is, $p-1$ is the smallest positive integer such that

$$\gamma^{p-1} \equiv 1 \bmod p.$$

(a) Prove that $\gamma^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Hint: $\gamma$ can be seen as a root of $T^{p-1} - \overline{1}$, where $p-1$ is even.

(b) Let $\delta$ be the multiplicative inverse of $\gamma$ modulo $p$. Prove that $\delta$ is a primitive root modulo $p$.

(c) Assume $\gamma'$ is another primitive root modulo $p$. Prove that $\gamma\gamma'$ is *not* a primitive root modulo $p$.

**Problem 9.3.**

(a) Let $f(T)$ be an irreducible polynomial modulo $p$, and consider any $a \in \mathbb{F}_p^\times$. Prove that $g(T) \coloneqq af(T)$ is also irreducible.

(b) Let $f(T)$ be a polynomial modulo $p$, a prime, of degree 2 or 3. Prove that $f(T)$ is irreducible if and only if $f(T)$ has no roots modulo $p$.

Hint: prove the contrapositive, look at the degrees of the factors of $f(T)$ and invoke a result from this section.

(c) Give an example illustrating why the reasoning in (b) does not help us determine if a given polynomial (modulo $p$) of degree $\geqslant 4$ is irreducible.

**Problem 9.4.** Consider two polynomials mod 5:

$$f(T) = T^3 + \overline{3}T^2 + \overline{2}T + 1$$

$$g(T) = \overline{2}T^4 + \overline{4}T^3 + T^2 + \overline{3}T + \overline{4}.$$

(a) Find the two polynomials mod $p$: $q(T)$ and $r(T)$, such that $\deg r < 3$ and

$$g(T) = f(T)q(T) + r(T).$$

(b) Apply the Division Algorithm to find the greatest common divisor of $f(T)$ and $g(T)$. Show your work. As in the case with integers, the gcd is the last non-zero remainder.

(c) Prove or disprove: The gcd that you have found in (b) is irreducible.

Hint: use Problem 9.3.

(d) Find the unique decompositions of $f(T)$ and $g(T)$ into irreducible polynomials mod $p$.

**Problem 9.5.** Find the smallest positive integer $a$ such that $2^a \equiv 11 \bmod p$, for the two primes: $p = 23$ and $p = 37$.

**Problem 9.6.** Find Alice and Bob's secret number $S$, if $g = 3,\ p = 17,\ A = 8$ and $B = 7$.

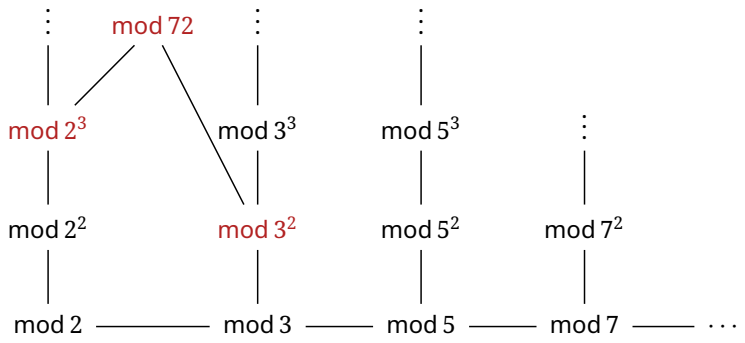
# 10. Assembling the Modular World

Back to the motivation of modular arithmetic.

(1) $x^2 + y^2 = 83$; we saw that it has no integer solutions by looking mod 4.

(2) $x^2 + y^2 = 3z^2$; we saw that it has only one rational solution $(0, 0, 0)$ by looking mod 3.

Each modulus only gives us partial information. In order to get a fuller picture, we want to assemble this information into one. In the horizontal direction we list all the primes, and in the vertical direction we list the prime powers.




We understand, for example, a given expression mod 72 by understanding the expression mod $2^3$ and mod $3^2$.

**Question** (Ancient Puzzle)**.** *There are an unknown number of oranges, fewer than* 100*.*

*If I group them in* 3*s, then* 2 *oranges are left.*

*If I group them in* 5*s, then* 3 *oranges are left.*

*If I group them in* 7*s, then* 2 *oranges are left.*

*How many oranges are there in total?*

**Translating the Ancient Puzzle:** *Suppose $N$ is an integer such that $0 < N \leqslant 100$, and*

$$N \equiv 2 \bmod 3, \quad N \equiv 3 \bmod 5, \quad N \equiv 2 \bmod 7$$

*What is $N$?*

## 10.1. The Chinese Remainder Theorem

**Notation.** Let $d, e$ be moduli and $a, b$ are integers. For any integer $x$, we write

$$x \equiv [a, b] \bmod [d, e], \quad \text{if } x \equiv a \bmod d \text{ and } x \equiv b \bmod e$$

For example, let $d = 3$, $e = 5$, then $67 \equiv [1, 2] \bmod [3, 5]$

**Theorem 10.1** (Chinese Remainder Theorem)**.** *Let $d$ and $e$ be moduli. Assume that $d$ and $e$ are coprime, that is* $\gcd(d, e) = 1$*. Then there's a one-to-one correspondence*

$$\underline{\mathrm{R}}(d) \times \underline{\mathrm{R}}(e) \longleftrightarrow \underline{\mathrm{R}}(de)$$

*where, recall $\underline{\mathrm{R}}(n) = \{0, 1, \ldots, n-1\}$ for an integer $n > 0$.*

*In particular, the system of congruences $X \equiv [a, b] \bmod [d, e]$ have a solution, unique* mod $de$*.*

**Example 10.2.** Let us assemble the congruences, i.e. solve for $N$ in the system of congruences

$$N \equiv [6, 2] \bmod [7, 5]$$

CRT (Theorem 10.1) tells us that a solution to this system exists. Computationally, we proceed as follows:

(1) Write each of the two congruences into integer equations

$$N \equiv 6 \bmod 7, \quad \text{if and only if} \quad N = 6 + 7x, \text{ for some integer } x$$
$$N \equiv 2 \bmod 5, \quad \text{if and only if} \quad N = 2 + 5y, \text{ for some integer } y$$

(2) Combine the two equations into one.

$$6 + 7x = N = 2 + 5y$$
$$7x - 5y = -4$$

(3) Find *one* particular solution using the division algorithm

$$7 = 5 \cdot 1 + 2 \qquad\qquad 1 = 5 - 2 \cdot 2$$
$$5 = 2 \cdot 2 + 1 \qquad\qquad = 5 - 2(7 - 5)$$
$$2 = 1 \cdot 2 + 0 \qquad\qquad = 7(-2) + 5(3)$$

So, we have

$$-4 = -4 \cdot 1 = -4(7(-2) + 5(3)) = 7(8) - 5(12).$$

Therefore we may take $(x, y) = (8, 12)$.

(4) Return to $N$. Our computations give us

$$N = 6 + 7x = 6 + 7(8) = 62$$

is a solution to $N \equiv [6, 2] \bmod [7, 5]$.

Finally, CRT (Theorem 10.1) tells us that the solution $N = 62$ is unique upto mod $7 \cdot 5$.

That is, if $M$ is another solution to $N \equiv [6, 2] \bmod [7, 5]$, then $M \equiv 62 \bmod 35 \equiv 27 \bmod 35$.

*Proof of Theorem 10.1 (CRT).* Consider the function

$$f : \underline{\mathsf{R}}(de) \to \underline{\mathsf{R}}(d) \times \underline{\mathsf{R}}(e), \quad N \mapsto ([N]_d, [N]_e),$$

where $[N]_d$ and $[N]_e$ are the natural representative of $N$ modulo $d$ and $e$ respectively. In particular,

$$[N]_d \equiv N \bmod d \quad \text{and} [N]_e \equiv N \bmod e$$

**Injectivity.** Assume $M, N \in \underline{\mathsf{R}}(de)$ are such that $f(M) = f(N)$. Let $(a, b) = f(M) = f(N)$. Then,

$$M \equiv [a, b] \bmod [d, e]$$
$$N \equiv [a, b] \bmod [d, e]$$
$$\text{Therefore, } M - N \equiv [0, 0] \bmod [d, e]$$

Hence, $d \mid (M - N)$ and $e \mid (M - N)$. Since $d$ and $e$ are coprime, by Problem 1.7

$$de \mid (M - N)$$

Hence, $M - N = 0$ or $|M - N| \geqslant de$.

Since $M, N \in \underline{\mathsf{R}}(de)$, we have $0 \leqslant M, N \leqslant de - 1$, this gives us

$$-(de - 1) \leqslant M - N \leqslant (de - 1).$$

That is, $|M - N| \leqslant de - 1 < de$. Thus, necessarily, $M - N = 0$. Therefore $f$ is injective.

**Bijectivity.** Note that $\#\underline{\mathsf{R}}(de) = de$ and $\#(\underline{\mathsf{R}}(d) \times \underline{\mathsf{R}}(e)) = \#\underline{\mathsf{R}}(d) \cdot \#\underline{\mathsf{R}}(e) = de$.

Therefore, $f$ is an injective map between two sets of the same size. Necessarily, $f$ is a bijection. □

**Remark 10.3.** Consider the map $f$ from the proof of Theorem 10.1, for coprime integers $d$ and $e$, which we showed implicitly to be surjective, by exhibiting it as a bijection. The surjectivity statement, accounting for injectivity, states:

$$\text{given } (a,b) \in \underline{\mathsf{R}}(d) \times \underline{\mathsf{R}}(e), \textit{ there exists a unique } N \in \underline{\mathsf{R}}(de) \text{ such that } f(N) = (a,b),$$

i.e., the system $X \equiv [a,b] \bmod [d,e]$ has a solution $X \equiv N \bmod de$.

In particular, the solution to the system $X \equiv [N,N] \bmod [d,e]$ is $X \equiv N \bmod de$.

**Remark 10.4.** One can use Theorem 10.1 to give another proof of the multiplicativity of the Euler totient function $\varphi$. One shows this by proving that the bijection $f$ in Theorem 10.1 restricts to a bijection

$$\underline{\mathsf{U}}(de) \longleftrightarrow \underline{\mathsf{U}}(d) \times \underline{\mathsf{U}}(e)$$

Comparing cardinalities, we obtain $\varphi(de) = \varphi(d)\varphi(e)$, whenever $\gcd(d,e) = 1$.

## 10.2. Applying CRT

(I) **More then two congruences.** Recall the ancient riddle: find the positive integer $N \leqslant 100$ such that

$$N \equiv 2 \bmod 3 \tag{$\leftmoon_1$}$$
$$N \equiv 2 \bmod 7 \tag{$\leftmoon_2$}$$
$$N \equiv 3 \bmod 5 \tag{$\leftmoon_3$}$$

*Solution.* From ($\leftmoon_1$) and ($\leftmoon_2$), we get that $N-2$ is divisible by 3 and 7. Since 3 and 7 are coprime, it follows that $N-2$ is divisible by $7 \cdot 3 = 21$. Hence, ($\leftmoon_1$) and ($\leftmoon_2$) give us

$$N \equiv 2 \bmod 21 \tag{$\leftmoon_4$}$$

We solve the simultaneous congruence given by ($\leftmoon_3$) and ($\leftmoon_4$). We rewrite them as

$$3 + 5x = N = 2 + 21y$$

for some integers $x, y$, giving us

$$5x - 21y = -1$$

An immediate solution is given by $(x,y) = (4,1)$ (alternatively, use the division algorithm). This gives us

$$N = 2 + 21(1) = 3 + 5(4) = 23$$

Now, CRT (Theorem 10.1) tells us that $N \equiv 23 \bmod 5 \cdot 21 \equiv 23 \bmod 105$ is the only solution modulo 105.

That is, the set of all positive solutions is $\{23 + 105k \ : \ k \in \mathbb{Z},\ k \geqslant 0\}$.

Since we were looking for $N \leqslant 100$, the answer is $N = 23$.

(II) **Quadratic Congruences.**

(IIa) Find all integers $0 \leqslant x \leqslant 34$ such that

$$x^2 \equiv 29 \bmod 35$$

**One method:** compute $0^2, 1^2, 2^2, \ldots, 34^2 \bmod 35$ and see if any one of them is $\equiv 29 \bmod 35$.

**A better method:** break $x^2 \equiv 29 \bmod 35$ into two congruences using the fact $35 = 5 \cdot 7$

$$\begin{cases} x^2 \equiv 29 \bmod 5 \equiv 4 \bmod 5 & (\text{✎}_5) \\ x^2 \equiv 29 \bmod 7 \equiv 1 \bmod 7 & (\text{✎}_7) \end{cases}$$

Since 5 and 7 are primes, we can use polynomial methods, i.e.

$$(\text{✎}_5) \text{ holds} \Leftrightarrow x^2 - \overline{4} = 0 \Leftrightarrow (x-\overline{2})(x+\overline{2}) = \overline{0}$$
$$\Leftrightarrow x = \overline{2} \text{ or } x = -\overline{2} = \overline{3}$$
$$\Leftrightarrow x \equiv 2 \bmod 5 \text{ or } x \equiv -2 \bmod 5$$

$$(\text{✎}_7) \text{ holds} \Leftrightarrow x^2 - \overline{1} = 0 \Leftrightarrow (x-\overline{1})(x+\overline{1}) = \overline{0}$$
$$\Leftrightarrow x = \overline{1} \text{ or } x = -\overline{1} = \overline{6}$$
$$\Leftrightarrow x \equiv 1 \bmod 7 \text{ or } x \equiv -1 \bmod 7$$

Therefore, we have four possibilities

| | $x \equiv 1 \bmod 7$ | $x \equiv 6 \bmod 7$ |
|---|---|---|
| $x \equiv 2 \bmod 5$ | Case 1 | Case 2 |
| $x \equiv 3 \bmod 5$ | Case 3 | Case 4 |

Let us consider Case 1, that is $x \equiv 1 \bmod 7$ and $x \equiv 2 \bmod 5$. Rewriting as

$$x = 1 + 7a \quad \text{and} \quad x = 2 + 5b$$

for some integer $a, b$, we obtain

$$7a - 5b = 1$$

An immediate solution is $(a, b) = (3, 4)$ (alternatively, use the division algorithm).

This tells us, $x = 1 + 7(3) = 22$. Hence the solution is $x \equiv 22 \bmod 35$.

Similar computations help us populate the table above, getting us:

| | $x \equiv 1 \bmod 7$ | $x \equiv 6 \bmod 7$ |
|---|---|---|
| $x \equiv 2 \bmod 5$ | $x \equiv 22 \bmod 35$ | $x \equiv 27 \bmod 35$ |
| $x \equiv 3 \bmod 5$ | $x \equiv 8 \bmod 35$ | $x \equiv 13 \bmod 35$ |

Thus, $x = 8,\ 13,\ 22,\ 27$ are the positive integers less than 35 whose square is $\equiv 29 \bmod 35$.

(IIb) Find all integers $0 \leqslant x \leqslant 34$ such that

$$x^2 \equiv 6 \bmod 35$$

Similarly, as in (IIa), let us break this congruence and observe that we have a solution

$$\Leftrightarrow \begin{cases} x^2 \equiv 6 \bmod 5 \\ x^2 \equiv 6 \bmod 7 \end{cases} \qquad \Leftrightarrow \begin{cases} x^2 \equiv 1 \bmod 5 \\ x^2 \equiv 6 \bmod 7 \end{cases} \qquad \Leftrightarrow \begin{cases} x \equiv 1 \bmod 5 \text{ or } x \equiv -1 \bmod 5 \\ \textbf{never happens} \end{cases}$$

Since, note that

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

Conclusion: for no positive integer $x$ do we have $x^2 \equiv 6 \bmod 35$.

## Problems

**Problem 10.1.** Prove that if $p$ is any prime and $a$ and $b$ are any nonzero integers such that $a \equiv b \bmod (p^2 - p)$, then $a^a \equiv b^b \bmod p$.

**Problem 10.2** (Lifting Multiplicative Inverses)**.** Let $p$ be a prime and $e > 0$ be an integer. Suppose $x, y$ are integer such that $xy \equiv 1 \bmod p^e$. Then $xy = 1 + p^e r$, for some integer $r$. Define

$$z = y - yrp^e$$

Verify that $z$ is a multiplicative inverse of $x$ modulo $p^{2e}$.

Find the multiplicative inverse of 3 modulo $5^8$ in $\underline{U}(5^8)$.

**Problem 10.3.** Solve the congruence equation $x^2 \equiv 17 \bmod 208$ by following the three steps:

(a) Solve the congruence equation $x^2 \equiv 17 \bmod 13$; more precisely, find $0 \leqslant x < 13$ that solves the given congruence.

(b) Solve the congruence equation $x^2 \equiv 17 \bmod 16$; more precisely, find $0 \leqslant x < 16$ that solves the given congruence.

(c) By combining (a) and (b) and then applying the Chinese Remainder Theorem, solve the congruence $x^2 \equiv 17 \bmod 208$; more precisely, find $0 \leqslant x < 208$ that solves the given congruence.

Note that $208 = 13 \cdot 16$ and $\gcd(13, 16) = 1$.

# 11. Quadratic Reciprocity

## 11.1. Quadratic Residues

**Definition 11.1.** Let $p$ be a prime and let $n$ be an integer.

- Say $n$, or $\overline{n}$, is a **quadratic residue (QR)** modulo $p$ if $n \equiv x^2 \bmod p$ for some integer $x$.
- Otherwise $n$, or $\overline{n}$, is called a **quadratic non-residue (QNR)**.

We can rephrase this in terms of polynomials: $n$ is a QR if and only if $T^2 - \overline{n} \in \mathbb{F}_p[T]$ is reducible.

For example, consider $p = 11$, we have

| $x \bmod 11$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{6}$ | $\overline{7}$ | $\overline{8}$ | $\overline{9}$ | $\overline{10}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $x^2 \bmod 11$ | $\overline{0}$ | $\overline{1}$ | $\overline{4}$ | $\overline{9}$ | $\overline{16} = \overline{5}$ | $\overline{25} = \overline{3}$ | $\overline{36} = \overline{3}$ | $\overline{49} = \overline{5}$ | $\overline{64} = \overline{9}$ | $\overline{81} = \overline{4}$ | $\overline{100} = \overline{1}$ |

Therefore, among $\mathbb{F}_{11} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{10}\}$,

the quadratic residues are: $\overline{0}, \overline{1}, \overline{4}, \overline{9}, \overline{5}, \overline{3}$; the quadratic non-residues are: $\overline{2}, \overline{6}, \overline{7}, \overline{8}, \overline{10}$.

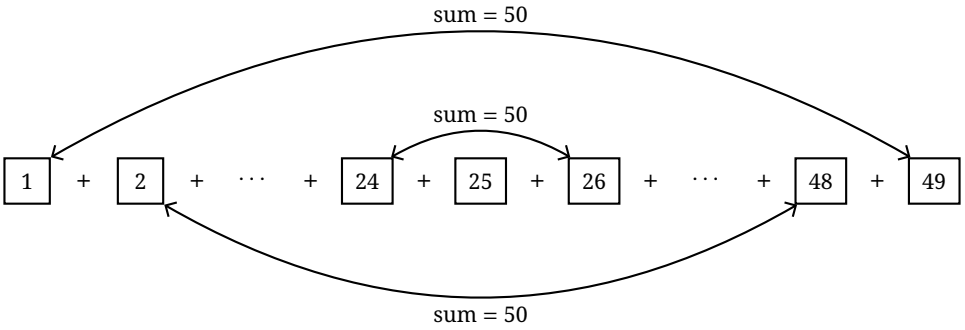
Hence, in $\underline{\mathsf{U}}(11) = \{1, 2, \ldots, 10\}$, we have *five* quadratic residues and *five* quadratic non-residues.

**Question.** *Given a prime $p$ and an integer $n$, can we determine whether $n$ is a QR modulo $p$?*

*Better yet, can we find an* effective algorithm *for this?*

## 11.2. The Idea of Partnership

**Example 11.2** (additive)**.** Let us compute $1 + 2 + 3 + \cdots + 49$.




Therefore,

$$(1 + 2 + 3 + \cdots + 49) = 50 \cdot (\#\,\text{pairs}) + 25 = 50 \cdot 24 + 25 = 1200 + 25 = 1225.$$

**Theorem 11.3** (Wilson's Theorem)**.** *Let $p$ be a prime number. Then we have*

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

*Proof.* Consider $\underline{\mathsf{U}}(p) = \{1, 2, \ldots, p-1\}$; we will partner elements as follows:

$$\textit{partner } x \in \underline{\mathsf{U}}(p) \textit{ with } y \in \underline{\mathsf{U}}(p) \textit{ if and only if } xy \equiv 1 \bmod p.$$

That is, partner $x$ with its multiplicative inverse $y$ modulo $p$. We know that any $x \in \underline{\mathsf{U}}(p)$ has a unique multiplicative inverse modulo $p$ in $\underline{\mathsf{U}}(p)$.

Before we proceed, let us determine when $x$ is its own partner. This occurs exactly when $x \cdot x \equiv 1 \bmod p$, i.e., when

$$x^2 - 1 \equiv 0 \bmod p$$

equivalently when it is a root of $T^2 - \overline{1} = (T - \overline{1})(T + \overline{1})$. Hence $x$ is its own partner when

$$x \equiv 1 \bmod p \quad \text{or} \quad x \equiv -1 \equiv p - 1 \bmod p$$

Thus, any $x \in \underline{\mathsf{U}}(p)$ is its own partner when $x = 1$ or $x = p - 1$.

Assume $p = 2$, then

$$(p-1)! = (2-1)! = 1! = 1 \equiv -1 \bmod 2$$

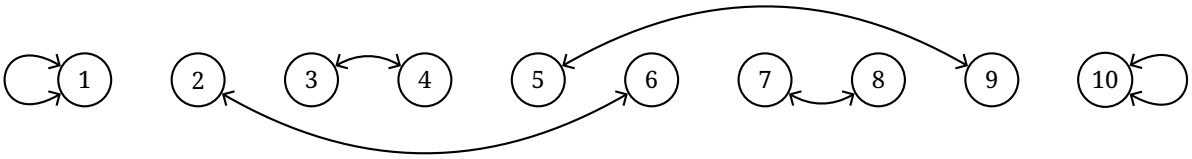
as claimed.

Assume now that $p$ is an odd prime. In this case, $\underline{\mathsf{U}}(p)$ contains two distinct elements, namely 1 and $p - 1$, that are self-partnered. All the other elements $x$ get partnered with some $y \neq x$. Therefore

$$\begin{aligned}(p-1)! &= \text{the product of all elements in } \underline{\mathsf{U}}(p) \\ &= 1 \cdot (p-1) \cdot (\text{partnered products}) \\ &\equiv (p-1) \cdot 1 \bmod p \\ &\equiv -1 \bmod p\end{aligned}$$

as claimed. □

For example, in the case $p = 11$, the partnership specified in the proof above is




**Proposition 11.4.** *Let $p$ be an odd prime, so $\#\underline{\mathsf{U}}(p) = p - 1$ is even. Then, exactly half of the elements of $\underline{\mathsf{U}}(p)$ are quadratic residues, the other half are quadratic non-residues.*

*Proof.* If $x \in \underline{\mathsf{U}}(p)$, then $p \nmid x^2$, so we have a function

$$\underline{\mathsf{U}}(p) \xrightarrow{f} \underline{\mathsf{U}}(p),\ x \mapsto [x^2]_p$$

Let $R$ be the image of $f$. By definition, $R$ is the set of quadratic residues in $\underline{\mathsf{U}}(p)$.

We claim that the function $f\colon \underline{\mathsf{U}}(p) \to R$ is a two-to-one function. That is, for any $a \in R$, there exist exactly two $x_1, x_2 \in \underline{\mathsf{U}}(p)$ such that $f(x_1) = a = f(x_2)$. Equivalently, $\#f^{-1}(a) = 2$.

Consider the polynomial $r(T) = T^2 - \overline{a} \in \mathbb{F}_p[T]$, for any $a \in R$, and let $y \in f^{-1}(a)$. Then $a = f(y)$, i.e.

$$y^2 \equiv a \bmod p, \quad \text{or equivalently} \quad r(\overline{y}) = 0.$$

Therefore, $f^{-1}(a)$ consists of roots of $r(T)$.

By definition of $R$, there's at least one $x_1 \in \underline{\mathsf{U}}(p)$ such that $a = f(x_1)$, i.e. $x_1^2 \equiv a \bmod p$, or equivalently $r(\overline{x}_1) = 0$.

Observe that $x_2 = p - x_1 \in \underline{\mathsf{U}}(p)$ also has this property,

$$\begin{aligned}x_2^2 = (p - x_1)^2 &\equiv (-x_1)^2 \bmod p \\ &\equiv x_1^2 \bmod p \\ &\equiv a \bmod p\end{aligned}$$

Since $\deg r = 2$, these two are necessarily its only roots. Furthermore, $x_1 \neq x_2$ as they have opposite parity, since $x_1 + x_2 = p$, an odd prime.

Hence, $\#f^{-1}(a) = 2$, as needed. Since $\#\Phi(p) = p-1$ and $f$ is two-to-one onto $R$. We have, $\#R = \dfrac{\#\underline{\mathsf{U}}(p)}{2} = \dfrac{p-1}{2}$. □

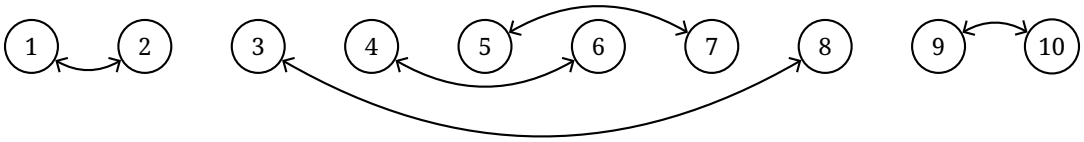
**Definition 11.5.** Let $p$ be a prime number and $a \in \underline{\mathsf{U}}(p)$. Say that $x, y \in \underline{\mathsf{U}}(p)$ are ***a*-partners** if

$$xy \equiv a \bmod p$$

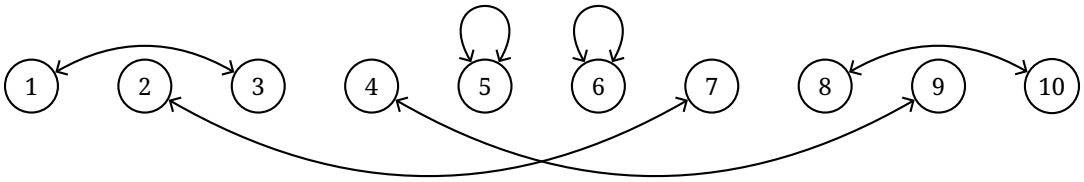
For example, let $p = 11$,

($a = 1$) this 1-partnership is what we used in the proof of Theorem 11.3; see diagram below the proof.

($a = 2$)




($a = 3$)




**Remark 11.6.** We note that every $x \in \underline{\mathsf{U}}(p)$ has an $a$-partner. Any such $x$ has a multiplicative inverse $z$ modulo $p$, i.e., $xz \equiv 1 \bmod p$. Then taking $y = [az]_p \in \underline{\mathsf{U}}(p)$ we have

$$xy \equiv x(az) = a(xz) \equiv a \bmod p$$

Hence $y$ is an $a$-partner of $x$.

## 11.3. Towards Quadratic Reciprocity

**Theorem 11.7** (Euler)**.** *Let $p$ be an odd prime, and let $a \in \underline{\mathsf{U}}(p)$. Then*

(1) *$a$ is a quadratic residue if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.*

(2) *$a$ is a quadratic non-residue if and only if $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.*

*Proof.* We first note that by Fermat's little theorem (Corollary 7.10) we have $a^{p-1} \equiv 1 \bmod p$.

Since $p$ is an odd prime, $p-1$ is even, so we get

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = a^{p-1} - 1 \equiv 0 \bmod p$$

if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p \quad \text{or} \quad a^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

From this, we note that the statements in the theorem are contrapositives of each other. Thus, it suffices to prove one of them; we prove (2).

($\Leftarrow$) If $a$ is a QNR, then there is *no* $x \in \underline{\mathsf{U}}(p)$ that is its own $a$-partner, because otherwise we have $x^2 = x \cdot x \equiv a \bmod p$ making $a$ a QR. Recall that every $x \in \underline{\mathsf{U}}(p)$ has an $a$-partner $y \in \underline{\mathsf{U}}(p)$, necessarily with $y \neq x$.

Hence, by Wilson's theorem (Theorem 11.3), we have

$$\begin{aligned} -1 &\equiv (p-1)! \bmod p \\ &\equiv (\text{product of elements in } \underline{\mathsf{U}}(p)) \bmod p \\ &\equiv (a\text{-partnered product}) \bmod p \\ &\equiv a^{\frac{p-1}{2}} \bmod p \end{aligned}$$

($\Rightarrow$) Suppose $a^{\frac{p-1}{2}} \equiv -1 \bmod p$ and for the sake of contradiction assume that $a$ is a QR, then there exists an $x \in \underline{\mathsf{U}}(p)$ such that $x^2 \equiv a \bmod p$. Then

$$\begin{aligned} x^{p-1} &= (x^2)^{\frac{p-1}{2}} \\ &\equiv a^{\frac{p-1}{2}} \bmod p \\ &\equiv -1 \bmod p \end{aligned}$$

contradicting Fermat's little theorem. Thus, necessarily, $a$ is a QNR. □

**Remark 11.8.** Note that Problem 9.1 (a) exactly says that a primitive root modulo $p$ is a quadratic non-residue.

**Example 11.9.** Determine whether $a = 3$ is a quadratic residue modulo $p = 43$.

*Answer.* We want to compute $3^{\frac{43-1}{2}} \bmod 43 = 3^{21} \bmod 43$. Note,

$$\begin{aligned} 3^1 &= 3 \bmod 43 \\ 3^2 &= 9 \bmod 43 \\ 3^4 &= 81 \equiv -5 \bmod 43 \\ 3^{16} &\equiv (-5)^4 \equiv 125 \cdot 5 \equiv (-4) \cdot 5 \equiv -20 \bmod 43 \end{aligned}$$

Therefore,

$$\begin{aligned} 3^{21} = 3^{16+4+1} &\equiv (-20) \cdot (-5) \cdot 3 \bmod 43 \\ &\equiv 100 \cdot 3 \bmod 43 \\ &\equiv 14 \cdot 3 \bmod 43 \\ &\equiv 42 \bmod 43 \\ &\equiv -1 \bmod 43 \end{aligned}$$

Hence, 3 is a QNR modulo 43.

**Example 11.10** (in-class)**.** Determine whether $a = 2$ is a quadratic residue modulo $p = 29$.

**Corollary 11.11.** *Let $p$ be an odd prime. Then*

$$-1 \textit{ is a quadratic residue } \bmod p \textit{ if and if } p \equiv 1 \bmod 4$$

*Equivalently, $T^2 + \overline{1} \in \mathbb{F}_p[T]$ is reducible if and only if $p \equiv 1 \bmod 4$.*

*Proof.* By Theorem 11.7, $-1$ is a QR mod $p$ if and only if

$$(-1)^{\frac{p-1}{2}} \equiv 1 \bmod p$$

Now,

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } \dfrac{p-1}{2} \text{ is even} \\ -1 & \text{if } \dfrac{p-1}{2} \text{ is odd} \end{cases}$$

Note that $\dfrac{p-1}{2}$ is even if and only if $p-1 = 4k$, for some integer $k$, if and only if $p \equiv 1 \bmod 4$. □

**Remark 11.12.** Suppose $p$ is a prime such that $p \equiv 1 \bmod 4$, then by Corollary 11.11, $-1$ is a QR modulo $p$.

Constructively, how does one find an integer $x$ such that $x^2 \equiv -1 \bmod p$? That it, a "square root of $-1 \bmod p$".

Consider

$$A = 1 \cdot 3 \cdot 5 \cdots (p-2)$$

$$B = 2 \cdot 4 \cdot 6 \cdots (p-3) \cdot (p-1)$$

Note that the multiplicands of $B$ are negatives of the multiplicands of $A$ modulo $p$. Therefore

$$A \equiv B(-1)^{\frac{p-1}{2}} \equiv B \bmod p$$

since $(p-1)/2$ is even. On the other hand,

$$AB = (p-1)! \equiv -1 \bmod p$$

Hence, $A^2 \equiv AB \equiv -1 \bmod p$.

For example, let $p = 13$, then $A = 1 \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot 11 \equiv 8 \bmod 13$. Therefore $x = 8$ is such that

$$x^2 = 64 \equiv -1 \bmod 13.$$

The other integer realising $-1$ as a QR is $y = 13 - 8 = 5$.

## 11.4. Legendre Symbol & Quadratic Reciprocity

**Definition 11.13.** Let $p$ be a prime number, and $a$ an integer. Then we define the **Legendre symbol** by the rule

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

**Important Observation.** If $a \equiv b \bmod p$, then

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

We rephrase Corollary 11.11 as follows

**Corollary 11.14** (Quadratic Reciprocity Law for $-1$)**.** *Let $p$ be an odd prime. Then*

$$\left(\frac{1}{p}\right) = 1, \quad \textit{for any } p$$

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

For example,

- $\left(\frac{3}{43}\right) = -1$, since 3 is a QNR modulo 43 (we computed $3^{\frac{43-1}{2}} \equiv -1 \bmod 43$).
- $\left(\frac{28}{29}\right) = \left(\frac{-1}{29}\right) = 1$, since $29 \equiv 1 \bmod 4$.
- $\left(\frac{39}{13}\right) = \left(\frac{0}{13}\right) = 0$.

Rephrasing Theorem 11.7 using the Legendre symbol.

**Theorem 11.15** (Euler)**.** *Let $p$ be an odd prime, and $a$ an integer. Then,*

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

*Note that $1 \not\equiv -1 \bmod p$ for odd primes.*

One non-trivial consequence of Theorem 11.15.

**Corollary 11.16.** *Let $p$ be an odd prime, and let $a, b$ be integers. Then*

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

*That is, $ab$ is a QR modulo $p$*

$$\Leftrightarrow \begin{cases} \textit{either } \text{both } a \textit{ and } b \textit{ are QR's} & \textit{(or)} \\ \textit{either } \text{both } a \textit{ and } b \textit{ are QNR's} \end{cases}$$

*Equivalently, $T^2 - \overline{ab} \in \mathbb{F}_p[T]$ is reducible if and only if both $T^2 - \overline{a}$, $T^2 - \overline{b}$ are reducible or both are irreducible.*

*Proof.* Suppose $p \mid a$ or $p \mid b$, then $p \mid ab$. Therefore,

$$\left(\frac{ab}{p}\right) = 0 = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Now, suppose $p \nmid a, b$. Then by Theorem 11.15, we have

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

But necessarily, both LHS and RHS are $\pm 1$.

Since $p$ is an odd prime, $1 \not\equiv -1 \bmod p$, therefore we can replace $\equiv$ with $=$ above. Thus,

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

□

For example, consider $p = 13,\ a = 2,\ b = 6$. Note,

$$2^{\frac{13-1}{2}} = 2^6 = 64 \equiv -1 \bmod 13; \qquad \left(\frac{2}{13}\right) = -1$$

$$\begin{aligned} 6^{\frac{13-1}{2}} = 6^6 = (6^2)^3 = 36^3 &\equiv (-3)^3 \bmod 13 \\ &\equiv -27 \bmod 13 \\ &\equiv -1 \bmod 13; \qquad \left(\frac{6}{13}\right) = -1 \end{aligned}$$

Therefore, both 2 and 6 are QNR modulo 13. On the other hand,

$$\left(\frac{2\cdot 6}{13}\right) = \left(\frac{12}{13}\right) = \left(\frac{-1}{13}\right) = 1,$$

since $13 \equiv 1 \bmod 4$. Therefore,

$$\left(\frac{2\cdot 6}{13}\right) = 1 = (-1)^2 = \left(\frac{2}{13}\right)\left(\frac{6}{13}\right)$$

**Theorem 11.17** (Quadratic Reciprocity Law for 2)**.** *Let $p$ be a prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 0 & \text{if } p = 2 \\ 1 & \text{if } p \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv \pm 3 \bmod 8 \end{cases}$$

*Proof.* If $p = 2$, the statement of the theorem follows from definition of the Legendre symbol.

So, assume $p$ is an odd prime.

Consider the following three subproducts of $(p-1)!$

$$A = 1\cdot 2\cdot 3\cdots\frac{p-3}{2}\cdot\frac{p-1}{2}, \qquad B = 2\cdot 4\cdot 6\cdots(p-3)\cdot(p-1), \qquad C = 1\cdot 3\cdot 5\cdots(p-4)\cdot(p-2)$$

There are three relations among $A$, $B$ and $C \bmod p$

(1) Each factor of $B$ is $2\times$ (a factor of $A$). Therefore

$$B = 2^{\frac{p-1}{2}}\cdot A$$

(2) Each factor of $C$ is negative mod $p$ a factor of $B$. Therefore

$$B \equiv (-1)^{\frac{p-1}{2}}\cdot C \bmod p$$

(3) In the product of $A$, replacing each even number $x$ by $p - x \equiv -x \bmod p$ and we will get $C$, so

$$C \equiv (-1)^{\#\text{replacements}}\cdot A \bmod p$$

Note that,

$$\#\text{replacements} = \#\text{even numbers in } 1,\ldots,\frac{p-1}{2} = \left\lfloor\frac{(p-1)/2}{2}\right\rfloor = \left\lfloor\frac{p-1}{4}\right\rfloor$$

Letting $D$ be the multiplicative inverse of $A$ modulo $p$ (since $p \nmid A$), we obtain

$$B = 2^{\frac{p-1}{2}}A \tag{1}$$

$$2^{\frac{p-1}{2}} \equiv BD \bmod p \tag{1'}$$

$$B \equiv (-1)^{\frac{p-1}{2}}C \bmod p \tag{2}$$

$$C \equiv (-1)^{\left\lfloor\frac{p-1}{4}\right\rfloor}A \bmod p \tag{3}$$

$$(-1)^{\left\lfloor\frac{p-1}{4}\right\rfloor} \equiv CD \bmod p \tag{3'}$$

Therefore, by Theorem 11.15

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

$$\underset{(1')}{\equiv} BD \bmod p$$

$$\underset{(2)}{\equiv} (-1)^{\frac{p-1}{2}} CD \bmod p$$

$$\underset{(3')}{\equiv} (-1)^{\frac{p-1}{2}} (-1)^{\left\lfloor \frac{p-1}{4} \right\rfloor} \bmod p$$

There are four possibilities of odd primes $p$ modulo 8, $p \equiv 1,\ 3,\ 5$ or $7 \bmod 8$

| $p$ | $\frac{p-1}{2}$ | $\left\lfloor \frac{p-1}{4} \right\rfloor$ | $\left(\frac{2}{p}\right)$ |
|---|---|---|---|
| $8k+1$ | $4k$ (even) | $2k$ (even) | 1 |
| $8k+2$ | $4k+1$ (odd) | $2k$ (even) | $-1$ |
| $8k+3$ | $4k+2$ (even) | $2k+1$ (odd) | $-1$ |
| $8k+4$ | $4k+3$ (odd) | $2k+1$ (odd) | 1 |

Therefore

$$\left(\frac{2}{p}\right) = \begin{cases} 0 & \text{if } p = 2 \\ 1 & \text{if } p \equiv 1, 4 \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv 2, 3 \equiv \pm 3 \bmod 8 \end{cases}$$

as claimed. □

For example, consider $p = 10337$. Observe $p = 10337 \equiv 337 \equiv 17 \equiv 1 \bmod 8$. Therefore

$$\left(\frac{2}{10337}\right) = 1$$

**Theorem 11.18** (The Quadratic Reciprocity Law; Gauss)**.** *Let $p$ and $q$ be odd primes. Then*

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

*That is, there is a tangible relation between the irreducibility of $T^2 - \overline{p} \in \mathbb{F}_\ell[T]$ and $T^2 - \overline{q} \in \mathbb{F}_p[T]$*

*Proof.* We will see two proofs for this cornerstone result in Sections 12 and 13. □

**Remark 11.19.** Gauss's Quadratic Reciprocity Law provides a very effective way to compute $\left(\frac{a}{p}\right)$.

For example, let us consider the questions: is $a = 3$ a quadratic residue modulo $p = 73$?

Equivalently, is the polynomial $T^2 - \overline{3} \in \mathbb{F}_{73}[T]$ irreducible?

We may employ three methods:

1. **(Brute Force)** Compute $x^2 \bmod 73$ for $x = 1, 2, \ldots, 72$ and see if $a = 3$ appears in the list.
   For a large primes ($p \sim 2^{4000}$) this is inefficient.
2. **(Euler's Theorem)** Compute $3^{\frac{73-1}{2}} \bmod 73$. Effective for computers.
3. **(Quadratic Reciprocity)**
$$\left(\frac{3}{73}\right) = (-1)^{\left(\frac{3-1}{2}\right)\left(\frac{73-1}{2}\right)}\left(\frac{73}{3}\right) = (-1)^{36}\left(\frac{1}{3}\right) = 1$$

Summarising,

**Theorem 11.20** (Quadratic Reciprocity Laws)**.** *Let $p$ be an odd prime*

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

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

(3) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$, *where $q$ is an odd prime $\neq p$*

**Example 11.21.** For which primes $p$ is 3 a quadratic residue modulo $p$?

*Answer.* Note that 3 is a QR mod $p$ for $p = 2$ and $p = 3$.

Therefore, now assume $p > 3$. Quadratic Reciprocity gives us

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

Note that

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv -1 \bmod 4 \end{cases} \qquad \text{and} \qquad \left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1 & \text{if } p \equiv 1 \bmod 3 \\ \left(\frac{-1}{3}\right) = -1 & \text{if } p \equiv -1 \bmod 3, \text{ since } 3 \not\equiv 1 \bmod 4 \end{cases}$$

Therefore

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

$$= \begin{cases} 1 & \text{if } p \equiv [1,1] \bmod [3,4] \\ 1 & \text{if } p \equiv [-1,-1] \bmod [3,4] \\ -1 & \text{if } p \equiv [5,5] \bmod [3,4] \\ -1 & \text{if } p \equiv [-5,-5] \bmod [3,4] \end{cases}$$

Assembling these congruences together using CRT (Remark 10.3), we find that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 12 \text{ or } p = 2 \\ -1 & \text{if } p \equiv \pm 5 \bmod 12 \end{cases}$$

For example, the smallest odd prime for which 3 is a quadratic residue is 11, since $11 \equiv -1 \bmod 12$,

$$6^2 \equiv 5^2 \equiv 3 \bmod 11,$$

and the smallest prime for which 3 is a quadratic non-residue is 7, since $7 \equiv -5 \bmod 12$. □

**Example 11.22.** Consider the polynomial $f(T) = T^2 - \overline{8}T + \overline{3} \in \mathbb{F}_p[T]$. For what primes $p$ is $f(T)$ irreducible?

*Answer.* First note that if $p = 2$,

$$f(T) = T^2 - \overline{8}T + \overline{3} = T^2 + \overline{1} = (T + \overline{1})^2.$$

Therefore $f(T)$ is reducible for $p = 2$.

Now, assume that $p$ is odd. Note that

$$\begin{aligned} f(T) &= T^2 - \overline{8}T + \overline{3} \\ &= T^2 - \overline{2} \cdot \overline{4}T + \overline{16} - \overline{13} \\ &= (T - \overline{4})^2 - \overline{13} \end{aligned}$$

Therefore, we see that $f(T)$ has a root if and only if $f(a) = 0$ for some $a \in \mathbb{F}_p$ if and only if $(a - \overline{4})^2 - \overline{13} = \overline{0}$ for some $a \in \mathbb{F}_p$ if and only if $\overline{13}$ is a square modulo $p$ if and only if 13 is a QR modulo $p$.

Hence, by Problem **??** and looking at the contrapositive, we have that $f(T)$ is irreducible if and only if 13 is a QNR modulo $p$ if and only if

$$\left(\frac{13}{p}\right) = -1$$

By the Quadratic Reciprocity laws, since $p$ is an odd prime, note that

$$\left(\frac{p}{13}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{13-1}{2}\right)}\left(\frac{13}{p}\right) = (-1)^{(p-1)\cdot 3}\left(\frac{13}{p}\right) = \left(\frac{13}{p}\right)$$

Thus $f(T)$ is irreducible if and only if $\left(\frac{p}{13}\right) = -1$.

We may necessarily assume that $p \neq 13$, and therefore $p \equiv \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6 \bmod 13$.

Since $13 \equiv 1 \bmod 4$, we have by the Quadratic Reciprocity laws

$$\left(\frac{-1}{29}\right) = 1, \qquad \text{therefore } \left(\frac{-x}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{x}{13}\right) = \left(\frac{x}{13}\right)$$

Therefore, necessarily, $p \not\equiv \pm 1 \bmod 13$ and it suffices to consider the cases where $p \equiv 2, 3, 4, 5, 6 \bmod 13$.

Since $13 \equiv -3 \bmod 8$ and $13 \equiv 1 \bmod 12$, we conclude by the Quadratic Reciprocity laws and Example 11.21 that

$$\left(\frac{2}{13}\right) = -1 \quad \text{and} \quad \left(\frac{3}{13}\right) = 1$$

Hence, we necessarily have $p \not\equiv \pm 3 \bmod 13$ but we may have $p \equiv \pm 2 \bmod 13$.

Thus, we are left with the case $p \equiv 4, 5, 6 \bmod 13$. Observe that,

$$\left(\frac{4}{13}\right) = \left(\frac{2}{13}\right)^2 = 1 \quad \text{and} \quad \left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = -1$$

Finally, applying the Quadratic Reciprocity laws

$$\left(\frac{5}{13}\right) = (-1)^{\left(\frac{5-1}{2}\right)\left(\frac{13-1}{2}\right)}\left(\frac{13}{5}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$$

since $5 \equiv 5 \bmod 12$ (Example 11.21).

Therefore, $f(T)$ is irreducible modulo $p$ if and only if $\left(\frac{p}{13}\right) = -1$ if and only if $p \neq 13$ is an odd prime such that

$$p \equiv \pm 2, \pm 5, \pm 6 \bmod 13$$ □

**Example 11.23.** Does the equation

$$x^2 = 59783y + 46,$$

where $59783 = 191 \cdot 313$, have any integer solutions?

*Answer.* We determine the answer as follows:

STEP 1. The division algorithm is very useful for linear equations, but this is a quadratic equation.

STEP 2. If there indeed was a solution, then reducing the equation modulo 59783

$$x^2 \equiv 46 \bmod 59783$$

would have an integer solution as well. Therefore, we focus on this congruence.

STEP 3. By CRT, $x^2 \equiv 46 \bmod 59783$ has a solution if and only if

$$\begin{cases} x^2 \equiv 46 \bmod 191; \text{ and} & (\text{🎁}_1) \\ x^2 \equiv 29 \bmod 313 & (\text{🎁}_2) \end{cases}$$

have solutions.

STEP 4. So, we look to see if (🎁$_1$) and (🎁$_2$) have an integer solutions, that is, compute

$$\left(\frac{46}{191}\right) \quad \text{and} \quad \left(\frac{46}{313}\right)$$

STEP 5. Observe that $\left(\frac{46}{191}\right) = \left(\frac{2}{191}\right)\left(\frac{23}{191}\right)$. Now, note that using the Quadratic Reciprocity laws, we have

$$\left(\frac{2}{191}\right) = 1 \qquad \text{since } 191 \equiv -1 \bmod 8$$

$$\begin{aligned} \left(\frac{23}{191}\right) &= (-1)^{\left(\frac{23-1}{2}\right)\left(\frac{191-1}{2}\right)}\left(\frac{191}{23}\right) \\ &= (-1)\left(\frac{7}{23}\right) \\ &= (-1)(-1)^{\left(\frac{7-1}{2}\right)\left(\frac{23-1}{2}\right)}\left(\frac{23}{7}\right) \\ &= (-1)^2\left(\frac{2}{7}\right) \\ &= 1 \qquad \text{since } 7 \equiv -1 \bmod 8 \end{aligned}$$

So, $\left(\frac{46}{191}\right) = 1 \cdot 1 = 1$. Therefore (🎁$_1$) has a solution.

STEP 6. Observe that $\left(\frac{46}{313}\right) = \left(\frac{2}{313}\right)\left(\frac{23}{313}\right)$. Now, note that using the Quadratic Reciprocity laws, we have

$$\left(\frac{2}{313}\right) = 1 \qquad \text{since } 313 \equiv 1 \bmod 8$$

$$\begin{aligned}
\left(\frac{23}{313}\right) &= (-1)^{\left(\frac{23-1}{2}\right)\left(\frac{313-1}{2}\right)}\left(\frac{313}{23}\right) \\
&= \left(\frac{14}{23}\right) \\
&= \left(\frac{2}{23}\right)\left(\frac{7}{23}\right) \\
&= \left(\frac{7}{23}\right) && \text{since } 23 \equiv -1 \bmod 8 \\
&= (-1)^{\left(\frac{7-1}{2}\right)\left(\frac{23-1}{2}\right)}\left(\frac{23}{7}\right) \\
&= (-1)\left(\frac{2}{7}\right) \\
&= -1 && \text{since } 7 \equiv -1 \bmod 8
\end{aligned}$$

So, $\left(\frac{46}{313}\right) = -1$. Therefore ($\text{🎁}_2$) does not have a solution.

Hence, necessarily, $x^2 \equiv 46 \bmod 59783$ has no integer solutions. Thus

$$x^2 = 59783y + 46$$

has no integer solutions. □

## 11.5. Application: Fermat's Christmas Theorem

**Theorem 11.24** (Fermat's Christmas Theorem)**.** *Let $p$ be a prime such that $p \equiv 1 \bmod 4$. Then the equation*

$$p = x^2 + y^2$$

*has integer solutions. That is, $p$ can be written as a sum of two squares.*

For example, $13 = 2^2 + 3^2$ and $17 = 4^2 + 1^2$. Of course, $p = 2 = 1^2 + 1^2$.

**Note.** This theorem called so since it appears in a letter by Fermat to Mersenne dated 25th Dec, 1640.

**Remark 11.25.**

- Suppose $p \equiv 3 \bmod 4$. Then $p$ cannot be written as a sum of two squares, since for integers $x, y$ we have $x^2 + y^2 \equiv 0, 1, 2 \bmod 4$.
- We consider the set of **Gaussian integers** $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. If $p \equiv 1 \bmod 4$, then

  $$p = (x + iy)(x - iy),$$

  for some integer $x, y$, in $\mathbb{Z}[i]$.

Our proof will be geometric. Before we give the proof, we build some geometric preliminaries. Hermann Minkowski is well-known for introducing such geometric ideas into number theory by developing a field called **geometry of numbers**.

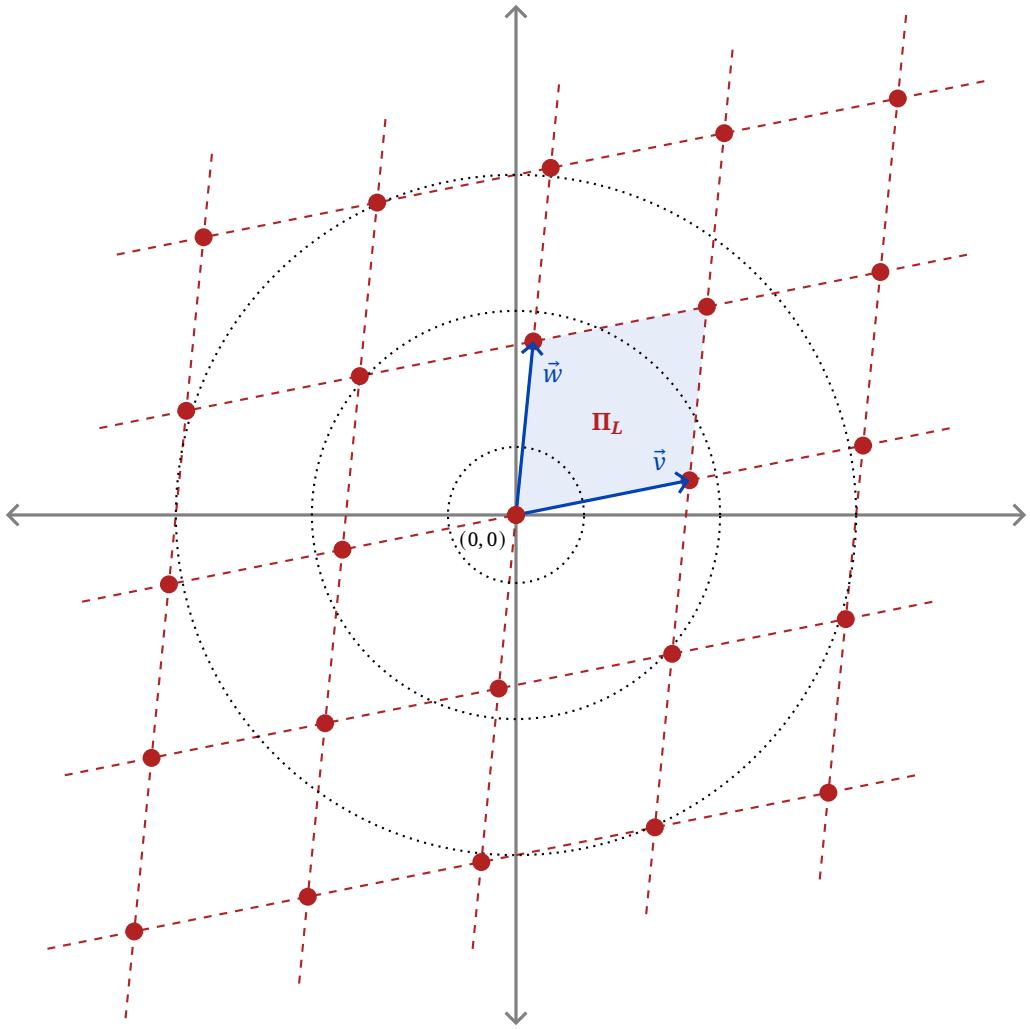
Consider a lattice, a parallelogram-grid of points in the plane; more precisely, fix the two non-parallel vector $\vec{v}$, $\vec{w}$ in the plane $\mathbb{R}^2$ and a **lattice** with basis $\vec{v}$, $\vec{w}$ is the set

$$L = \left\{a\vec{v} + b\vec{w} \ : \ a, b \in \mathbb{Z}\right\}$$

Associated to $L$ is its **fundamental parallelogram** (or **domain**), given as

$$\Pi_L = \left\{s\vec{v} + t\vec{w} \ : \ s, t \in [0, 1]\right\}.$$

For example,




Now, consider $C_r$'s, circles of radius $r$ centred at the origin.

1. If $r$ is very small, the only grid point contained in the circle will be the origin.
2. If $r$ is sufficiently large, the circle will contain grid points other than the origin.

**Question.** *When can we be sure that a circle of radius $r$ centred at the origin contains a grid point other than the origin? We are seeking for an answer that depends on $r$.*

A possible answer can be to take $r > \min\left\{|\vec{v}|, |\vec{w}|\right\}$; a more useful characterisation, for the purposes of proving Theorem 11.24, is given as follows.

**Theorem 11.26** (Minkwoski). *If* $\text{Area}(C_r) = \pi r^2 > 4 \cdot \text{Area}(\Pi_L)$*, then* $C_r$ *contains at least one grid point* $\neq (0,0)$.

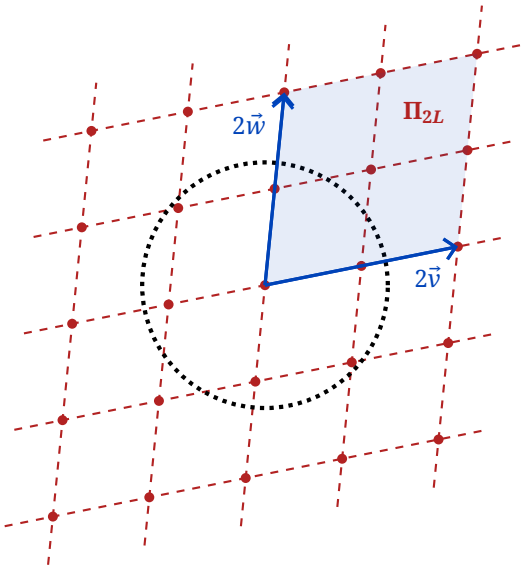
*Proof.* Let $L$ and $C_r$ be as in the statement, i.e., $L$ is a lattice with some basis $\vec{v}, \vec{w} \in \mathbb{R}^2$ with fundamental domain $\Pi_L$ and $C_r$ is a circle of radius $r$ centred at $(0,0)$ such that $\text{Area}(C_r) = \pi r^2 > 4 \cdot \text{Area}(\Pi_L)$.

Consider the lattice $2L$, the lattice with basis $2\vec{v}$ and $2\vec{w}$ which has the fundamental domain

$$\Pi_{2L} = \left\{ s(2\vec{v}) + t(2\vec{w}) \ : \ s,t \in [0,1] \right\}.$$

Furthermore, $\text{Area}(\Pi_{2L}) = 4 \cdot \Pi_L$. Therefore the assumption may be restated as $\text{Area}(C_r) = \pi r^2 > \text{Area}(\Pi_{2L})$.

For example, you may visualise this as follows, where we have $C_r$, the lattice $L$ and the funamental domain $\Pi_{2L}$.



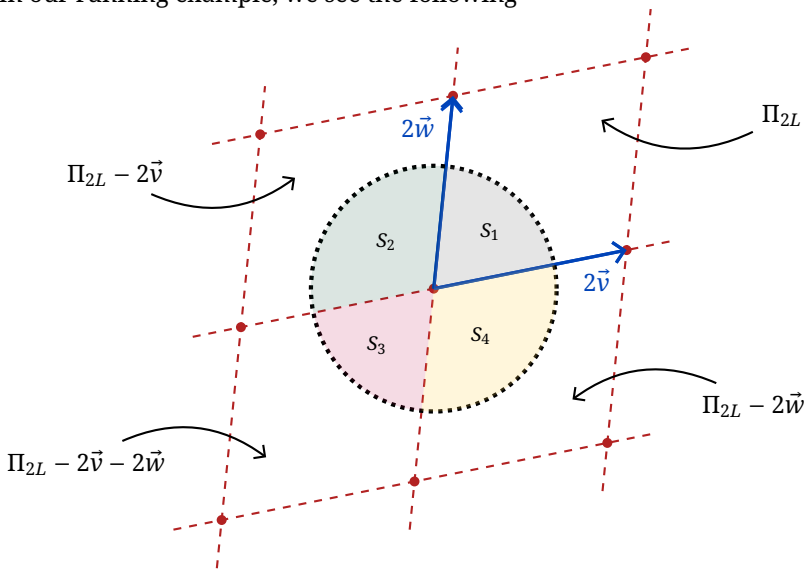

All of $\mathbb{R}^2$ is tessellated by translates of $\Pi_{2L}$ by elements of the lattice $2L$, i.e.,

$$\mathbb{R}^2 = \bigcup_{\ell \in 2L} (\Pi_{2L} + \ell)$$

Define the *sector* $S_\ell$ associated to $\ell \in 2L$ to be the intersection

$$S_\ell = C_r \cap (\Pi_{2L} + \ell)$$

In our running example, we see the following




$$\begin{aligned} S_1 &= S_{\vec{0}} \\ &= C_r \cap \Pi_{2L} \end{aligned}$$

$$\begin{aligned} S_2 &= S_{-2\vec{v}} \\ &= C_r \cap (\Pi_{2L} - 2\vec{v}) \end{aligned}$$

$$\begin{aligned} S_3 &= S_{-2\vec{v}-2\vec{w}} \\ &= C_r \cap (\Pi_{2L} - 2\vec{v} - 2\vec{w}) \end{aligned}$$

$$\begin{aligned} S_4 &= S_{-2\vec{w}} \\ &= C_r \cap (\Pi_{2L} - 2\vec{w}) \end{aligned}$$

Let $\ell_1, \ldots, \ell_t$ be those elements of $2L$ such that

$$C_r = \bigsqcup_{i=1}^{t} S_{\ell_i}$$

In particular, $\text{Area}(C_r) = \sum_{i=1}^{t} \text{Area}(S_{\ell_i})$.

We may translate each sector in $\Pi_{2L}$ by considering

$$T_{\ell_i} \coloneqq S_{\ell_i} - \ell_i$$

Necessarily $\text{Area}(T_{\ell_i}) = \text{Area}(S_{\ell_i})$. Therefore, $T_{\ell_i} \subseteq \Pi_{2L}$ and

$$\text{Area}(C_r) = \sum_{i=1}^{t} \text{Area}(T_{\ell_i})$$

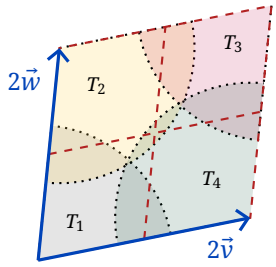
By assumption,

$$\text{Area}(\Pi_{2L}) < \text{Area}(C_r) = \sum_{i=1}^{t} \text{Area}(T_{\ell_i})$$

Therefore, there must be overlap amongst the translated sectors $T_{\ell_i}$'s within $\Pi_{2L}$.

In our running example, $\ell_1 = \vec{0},\ \ell_2 = -2\vec{v},\ \ell_3 = -2\vec{v} - 2\vec{w}$ and $\ell_4 = -2\vec{w}$. Define $T_i \coloneqq T_{\ell_i}$.

The fundamental domain, with the the translated sectors, looks like as follows, illustrating the overlap:




Let $T_{\ell_i}$ and $T_{\ell_j}$, for some $1 \leqslant i \neq j \leqslant t$, be the two translated sectors that overlap, i.e., intersect non-trivially. Let

$$x \in T_{\ell_i} \cap T_{\ell_j} = (S_{\ell_i} - \ell_i) \cap (S_{\ell_j} - \ell_j)$$

Therefore, $x = P - \ell_i = Q - \ell_j$ for some $P \in S_{\ell_i} \subseteq C_r$ and $Q \in S_{\ell_j} \subseteq C_r$.

Since $\ell_i, \ell_j \in \Pi_{2L}$, we may write $\ell_i = 2a_i\vec{v} + 2b_i\vec{w}$ and $\ell_j = 2a_j\vec{v} + 2b_j\vec{w}$.

Therefore,

$$\frac{P - Q}{2} = \frac{\ell_i - \ell_j}{2} = (a_i - a_j)\vec{v} + (b_i - b_j)\vec{w} \eqqcolon \vec{y}$$

Note that $\vec{y} \neq (0,0)$ since $\ell_i \neq \ell_j$ and $\vec{y} \in L$. While, $(P - Q)/2 \in C_r$ since $P, Q \in C_r$ and $C_r$ is convex.

Thus, $(0,0) \neq \vec{y} \in L \cap C_r$, as desired. □

We are now ready to prove Fermat's Christmas Theorem.

*Proof of Fermat's Christmas Theorem (Theorem 11.24).* Assume $p$ is a prime such that $p \equiv 1 \bmod 4$.

By the Quadratic Reciprocity Laws, we know $-1$ is a QR modulo $p$.

Therefore, there exists an integer $n$ such that $n^2 \equiv -1 \bmod p$.

Consider the set $L = \left\{(x, y) \in \mathbb{Z}^2 \ : \ x \equiv ny \bmod p\right\}$. We claim that $L$ is a lattice with basis $\vec{v} = (n, 1)$ and $\vec{w} = (p, 0)$.

**Claim.** $L$ is a lattice with basis $\vec{v} = (n, 1)$ and $\vec{w} = (p, 0)$.

More precisely, any $(x, y) \in L$ can be uniquely written as

$$(x, y) = a\underbrace{(n, 1)}_{\vec{v}} + b\underbrace{(p, 0)}_{\vec{w}}, \quad \text{for some } a, b \in \mathbb{Z}$$

and conversely, for any $a, b \in \mathbb{Z}$, we have $a\vec{v} + b\vec{w} \in L$.

*Proof of Claim.* If $(x, y) \in L$, necessarily $x \equiv ny \bmod p$. Therefore, we may write

$$x = ny + pz,$$

for some integer $z$. Taking $a = y$ and $b = z$, we see that

$$a(n, 1) + b(p, 0) = y(n, 1) + z(p, 0) = (ny, y) + (pz, 0) = (ny + pz, y) = (x, y),$$

as needed.

We will now show that $a = y$ and $b = z$ are unique such integers.

Assume that there exist integers $c, d$ such that $(x, y) = c(n, 1) + d(p, 0)$. Then, $x = nc + pd$ and $y = c$.

We immediately obtain $a = y = c$. Moreover,

$$pd = x - nc = x - ny = pz$$

Necessarily, $d = z = b$.

Conversely, for any $a, b \in \mathbb{Z}$, consider

$$(x, y) = a\vec{v} + b\vec{w} = (an + bp, a);$$

i.e. $x = an + bp$ and $y = a$. Therefore, $x = an + bp \equiv na \equiv ny \bmod p$. Hence, $(x, y) \in L$. □

We may now assume that $L$ has basis $\vec{v} = (n, 1)$ and $\vec{w} = (p, 0)$. Therefore,

$$\text{Area}(\Pi_L) = \left|\det(\vec{v}, \vec{w})\right| = \left|\det\begin{pmatrix} n & p \\ 1 & 0 \end{pmatrix}\right| = p$$

Let us consider the circle of area $4p + \varepsilon$ for some small $\varepsilon > 0$. That is, we consider a circle $C_r$ centred at $(0, 0)$ with radius

$$r = \sqrt{\frac{4p + \varepsilon}{\pi}}$$

By assumption, we have $\text{Area}(C_r) > 4 \cdot \text{Area}(\Pi_L)$. Hence, by Theorem 11.26, there exists an $(0, 0) \neq (x, y) \in L \cap C_r$.

Thus,

$$0 < x^2 + y^2 \leqslant r^2 = \frac{4p + \varepsilon}{\pi}, \quad \text{since } (x, y) \in C_r \tag{📢1}$$

$$x \equiv ny \bmod p, \quad \text{since } (x, y) \in L \tag{📢2}$$

From (📢2), we have $x^2 \equiv n^2y^2 \equiv -y^2 \bmod p$, since $n^2 \equiv -1 \bmod p$. Hence, $x^2 + y^2 \equiv 0 \bmod p$. In particular,

$$\frac{x^2 + y^2}{p} \in \mathbb{Z}$$

From (📢1), we have

$$0 < \frac{x^2 + y^2}{p} \leqslant \frac{1}{p} \cdot \frac{4p + \varepsilon}{\pi} = \frac{4}{\pi} + \frac{\varepsilon}{\pi p} \tag{💎}$$

Our choice of $\varepsilon$ has been arbitrary, let us make it slightly concrete by having chosen an $\varepsilon < \pi p/2$, since then

$$\frac{4}{\pi} + \frac{\varepsilon}{\pi p} < \frac{4}{\pi} + \frac{1}{2} < 2 \tag{🚗}$$

Thus, from (💎) and (🚗), conclude

$$0 < \frac{x^2 + y^2}{p} < 2, \quad \text{where } \frac{x^2 + y^2}{p} \in \mathbb{Z}$$

Necessarily, $\dfrac{x^2 + y^2}{p} = 1$, and therefore $p = x^2 + y^2$. □

**Remark 11.27.** Let

$$\Sigma_2 = \left\{x \in \mathbb{Z} \,:\, x = a^2 + b^2, \text{ for some } a, b \in \mathbb{Z}\right\},$$

that is, it is the set of integers that can be written as a sum of two squares.

Theorem 11.24 tells us that a prime $p \in \Sigma_2$ if and only if $p \equiv 1 \bmod 4$.

Now, one can verify the following identity directly

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2; \tag{✳}$$

which tell us that if $x,\ y \in \Sigma_2$, then $xy \in \Sigma_2$.

Noting that if a prime $q \equiv 3 \bmod 4$ then $q \notin \Sigma_2$, we get a complete description of $\Sigma_2$.

$$x \in \Sigma_2 \Leftrightarrow \text{every prime } q \equiv 3 \bmod 4 \text{ divides } x \text{ to an even power (take it to be 0 if } q \nmid x)$$

For example, $195 = 3 \cdot 5 \cdot 13$ is not a sum of two squares, since the exponent of 3 in the factorisation is odd.

However, $585 = 3^2 \cdot 5 \cdot 13$ is a sum of two squares.

To express it as such, we first write 5 and 13 as sums of two squares:

$$5 = 1^2 + 2^2 \quad \text{and} \quad 13 = 2^2 + 3^2.$$

First, using the identity (✳) we may write $65 = 5 \cdot 13$ as a sum of two squares

$$5 \cdot 13 = (1^2 + 2^2)(2^2 + 3^2) = (1 \cdot 2 - 2 \cdot 3)^2 + (1 \cdot 3 + 2 \cdot 2)^2 = 4^2 + 7^2$$

Finally multiplying throughout $3^2$ we get

$$\begin{aligned} 585 = 3^2 \cdot 5 \cdot 13 &= 3^2 \cdot (1^2 + 2^2) \cdot (2^2 + 3^2) \\ &= 3^2 \cdot (4^2 + 7^2) \\ &= (3 \cdot 4)^2 + (3 \cdot 7)^2 \\ &= 12^2 + 21^2 \end{aligned}$$

That is, $585 = 12^2 + 21^2$.

**Remark 11.28.** Initiating a set-up similar to the one we had while proving Theorem 11.24, this time in $\mathbb{R}^4$, and using a version of Theorem 11.26 in four dimensions with a three-dimensional sphere and four-dimensional lattice, again by Minkowski, allows us to prove the following celebrated theorem.

**Theorem** (Lagrange's Four-Square Theorem)**.** *Let $n$ be a positive integer. Then the equation*

$$n = x^2 + y^2 + z^2 + w^2$$

*has integer solutions. That is, any positive integer $n$ can be written as a sum of four squares.*

## Problems

**Problem 11.1.** We will see how ideas of partnership can give new proofs of two results we have seen before.

(a) Problem 2.5 (b) states: *$n$ is a square-free number if and only if it has odd-many positive divisors.*

Prove the statement by establishing some form of partnership between certain pairs in the set $\mathscr{D}(n)$.

(b) Problem 8.1 states: *$\varphi(n)$ is even, for any integer $n > 2$.*

Prove the statement by establishing some form of partnership between certain pairs in the set $\underline{\mathsf{U}}(n)$.

**Problem 11.2.** Let $p$ be an odd prime. Recall that a primitive root modulo $p$ is an integer $\gamma$ such that

$$\gamma^{p-1} \equiv 1 \bmod p \quad \text{and} \quad \gamma^e \not\equiv 1 \bmod p \text{ for } 0 < e < p-1$$

Some results that we proved in this lecture can be proved via the existence of $\gamma$ (Theorem 9.20).

(a) Consider $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{\overline{0}\}$ and let $\gamma$ be a primitive root. Prove that

$$\mathbb{F}_p^\times = \left\{[\gamma^e]_p \ : \ 0 \leqslant e < p-1\right\}$$

(b) Use a primitive root $\gamma$ to demonstrate that $-1$ is a QR modulo $p$ if and only if $p \equiv 1 \bmod 4$.

(c) Use a primitive root $\gamma$ to prove Theorem 11.3, by first showing that

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

(d) Given a primitive root $\gamma$, and an integer $a$ such that $a \not\equiv 0 \bmod p$, prove that

$$a \text{ is a QR modulo } p \text{ if and only if } a \equiv g^e \bmod p \text{ for an even number } e.$$

Use this to prove Euler's theorem (Theorem 11.7).

**Problem 11.3.** Consider the polynomial

$$f(T) = T^2 - \overline{6}T + \overline{4} \in \mathbb{F}_p[T], \quad \text{where } p \text{ is a prime.}$$

In this problem, we will determine the primes for which $f(T)$ is irreducible.

(a) "Completing the square", rewrite $f(T)$ as

$$f(T) = (T - \overline{a})^2 - \overline{q},$$

for some integer $a$ and prime $q$.

(b) Argue that $f(T)$ has no roots if and only if $q$ is a quadratic non-residue modulo $p$.

Equivalently, that $f(T)$ is irreducible if and only if

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

(c) Using Quadratic Reciprocity, reduce this question to determining $\left(\frac{p}{q}\right)$.

Determine this by considering cases given by possibilities for $p \bmod q$ and other Quadratic Reciprocity Laws.

(d) Conclude. Your answer should look something like

$$f(T) \text{ is irreducible} \quad \text{if and only if} \quad p \equiv _____ \bmod q.$$

**Problem 11.4.** For which primes $p$ is 5 a quadratic residue modulo $p$?

**Problem 11.5.** If $n = 3^{e_3}5^{e_5}7^{e_7}\cdots$ is an *odd* positive integer, and $a$ is an integer, the **Jacobi symbol** is defined as

$$\left(\frac{a}{n}\right) \coloneqq \left(\frac{a}{3}\right)^{e_3} \cdot \left(\frac{a}{5}\right)^{e_5} \cdot \left(\frac{a}{7}\right)^{e_7} \cdots$$

where $\left(\frac{a}{p}\right)$ is the usual Legendre symbol. Prove the following properties.

(a) If $a \equiv b \bmod n$, then

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

(b) Prove that

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \gcd(a,n) \neq 1 \\ \pm 1 & \gcd(a,n) = 1 \end{cases}$$

(c) If $a,\ b$ are integers, then

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

(d) If $m,\ n$ are coprime odd positive integers, then

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

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

(f) Prove that if $a$ is a quadratic residue modulo $n$ and $\gcd(a,n) = 1$, then $\left(\frac{a}{n}\right) = 1$.

(g) Unlike the Legendre symbol, the converse of (f) does not hold for the Jacobi symbol. That is,

$$\text{if } \left(\frac{a}{n}\right) = 1 \text{ and } \gcd(a,n) = 1, \text{ then } a \text{ is not necessarily a quadratic residue modulo } n$$

Verify this with $n = 15$ and $a = 2$.

# 12. Proof of Quadratic Reciprocity à la Zolotarev

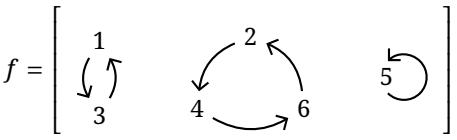
## 12.1. Permutations & their Sign

**Definition 12.1** (Permutation)**.** A **permutation** of a (finite) set $S$ is a *bijection* $f : S \to S$.

**Example 12.2.** Consider $S = \{1, 2, 3, 4, 5, 6\}$, and let a permutation $f$ be given by the rule

$$f(1) = 3 \qquad f(2) = 4 \qquad f(3) = 1 \qquad f(4) = 6 \qquad f(5) = 5 \qquad f(6) = 2$$

This is best visualised, for our purposes, using a *cycle* diagram

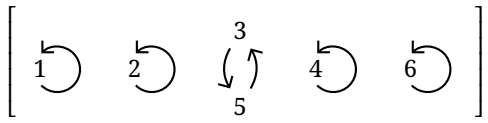
$f =$ 


So $f$ consists of

- 1 cycle of length 2;
- 1 cycle of length 3; and
- 1 cycle of length 1.

**Definition 12.3.** A **transposition** of $S$ is a permutation that *exchanges two distinct elements* in $S$ and fixes the rest. That is, in cycle notation, it consists of exactly 1 cycle of length 2 and every other cycle has length 1.

**Example 12.4.** Consider $S = \{1, 2, 3, 4, 5, 6\}$, and a transposition is

$\tau =$ 


We use the notation $\tau = (3\ 5) = \tau_{3,5}$.

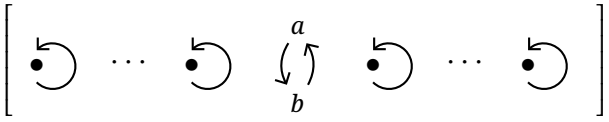
**Definition 12.5** (Characterisation 1 of Sign)**.** Let $S$ be a finite set and $f$ a permutation.

- ▷ The **sign of a cycle** of length $\ell$ is defined to be $(-1)^{\ell-1}$.
- ▷ The **sign of a permutation** $f$, denoted $\mathrm{sgn}(f)$, is the product of the signs of the cycle in $f$.

**Example 12.6.**

- Any transposition has sign $= -1$.

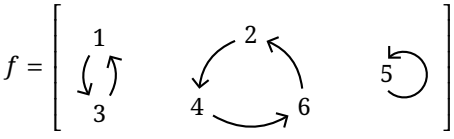
  Consider the following transposition

  $\tau_{a,b} =$ 


  has 1 cycle of length 2 and therefore has sign $(-1)^{2-1} = -1$, while the remaining cycles have length 1 and hence their sign is $(-1)^{1-1} = +1$. The product of these signs is $-1$, i.e.,

  $$\mathrm{sgn}(\tau_{a,b}) = -1.$$

- Consider the following permutation

  $f =$ 

So, we have

$$\operatorname{sgn}(f) = (-1)^{2-1} \cdot (-1)^{3-1} \cdot (-1)^{1-1} = (-1) \cdot (+1) \cdot (+1) = -1$$

**Lemma 12.7.** *Let $g$ and $f$ be permutations of a set $S$, then their composition $g \circ f$ is also a permutation.*

*Proof.* Composition of bijective functions is bijective. □

**Example 12.8.** It is important to recall and remember that generally $f \circ g \neq g \circ f$, where $f$ and $g$ are permutations. Let $g = \tau_{1,2}$ and $f = \tau_{2,3}$ be transpositions of $S = \{1, 2, 3\}$, then

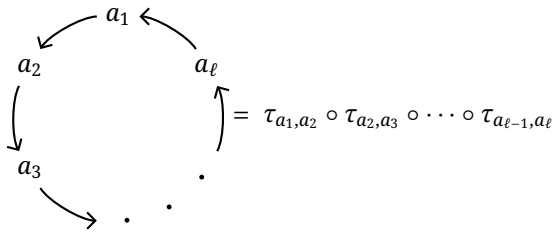



**Proposition 12.9.** *Let $S$ be a finite set. Every permutation of $S$ is an iterated composition of transpositions.*

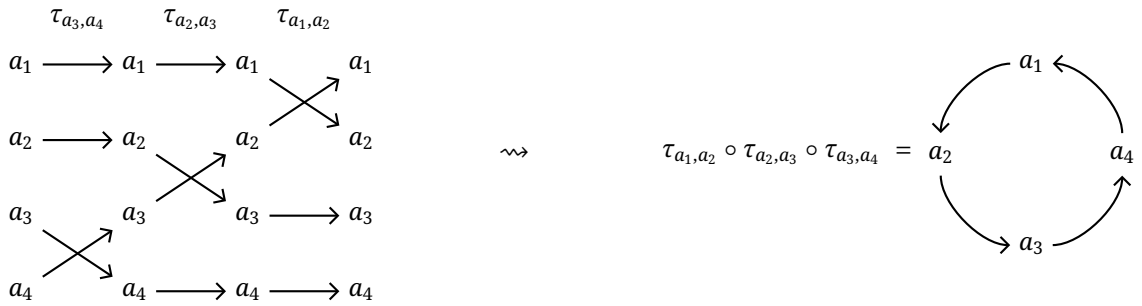
*Proof Sketch.* Let $f$ be a permutation. Writing it in cycle notation

$$f = [C_1 \quad C_2 \quad \cdots \quad C_r], \quad \text{we have } f = C_1 \circ C_2 \circ \cdots \circ C_r,$$

where a cycle $C_i$ is treated as a permutation of $S$ by fixing elements that do not appear in the cycle.
So, it is enough to show that any cycle is a composition of transpositions. One then has




As an example, consider the case $\ell = 4$; the general case looks similar.




□

**Discussion 12.10.** Let us investigate what occurs when we compose a permutation $f$ with a transposition $\tau$.
On a finite set $S$, assume $\tau = \tau_{a,b} = (a\ b)$ and we consider $\tau \circ f$. We have three cases: in the cycle diagram of $f$

**Case (1)** $a$ and $b$ do not belong to any cycle of $f$; or

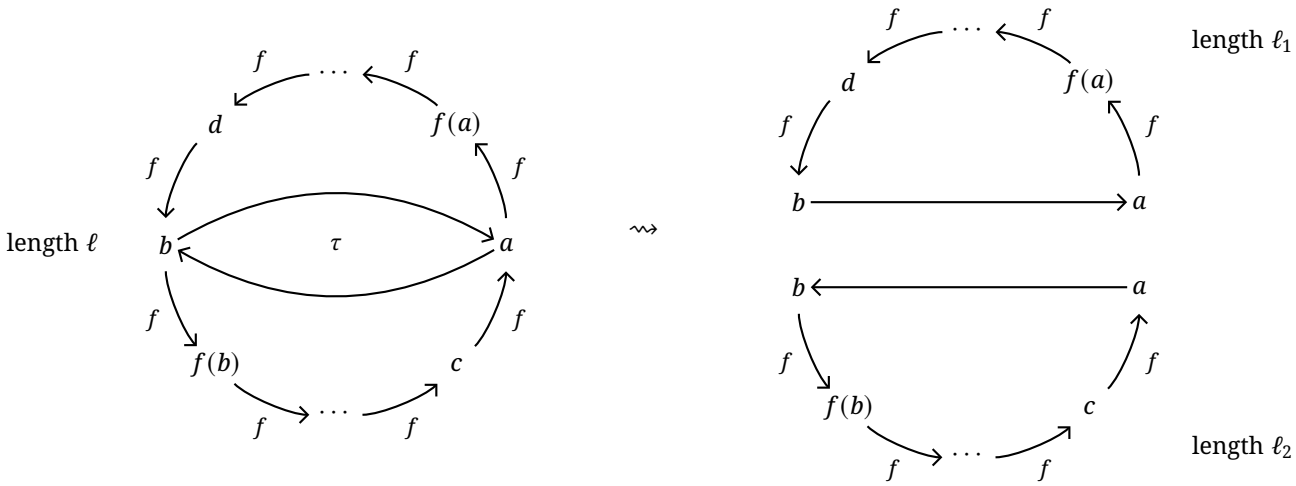
**Case (2)** $a$ and $b$ belong to the same cycle of $f$; or

**Case (3)** $a$ and $b$ belong to different cycles of $f$.

Case (1) is the simplest, since in this case the cycle diagram of the composition $\tau \circ f$ is one where we append $\tau$ to the cycle diagram of $f$ and nothing else changes.

$$\tau \circ f = \left[ \begin{array}{cc} a & \\ \circlearrowleft & f \\ b & \end{array} \right]$$

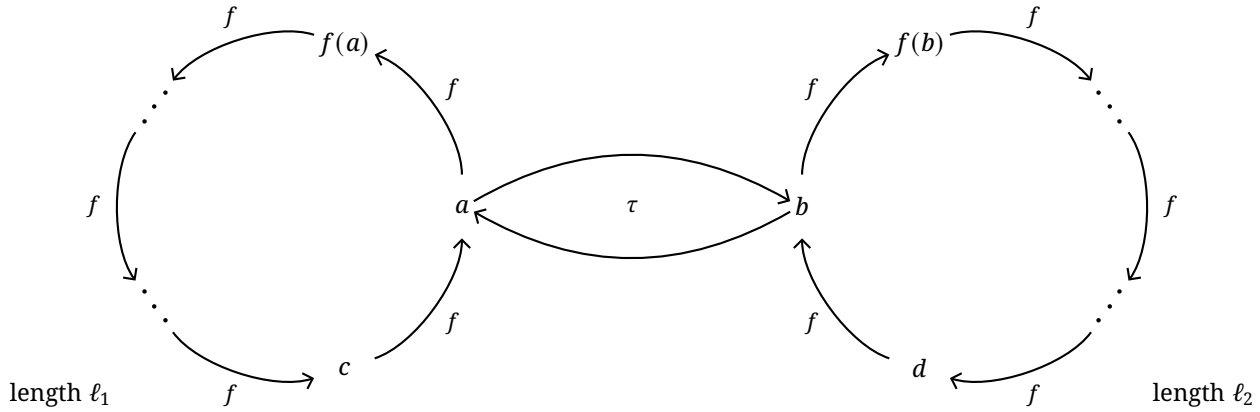
In Case (2), we have the following for $\tau \circ f$

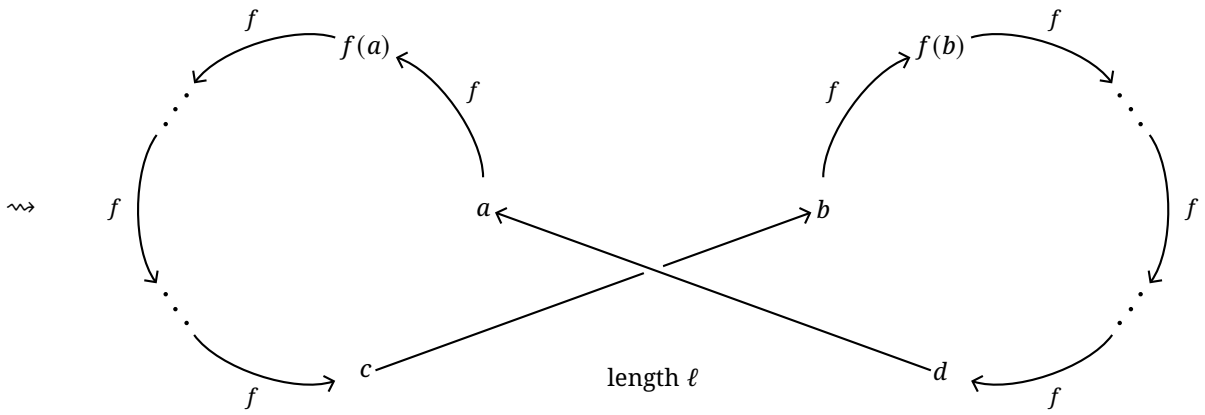



Therefore in Case (2), composing with $\tau$ on the left *breaks the single cycle* in $f$, of length $\ell$, *into two cycles* of $\tau \circ f$ of respective lengths $\ell_1$ and $\ell_2$ with

$$\ell = \ell_1 + \ell_2$$

In Case (3), we have the following for $\tau \circ f$






Therefore in Case (3), composing with $\tau$ on the left *merges the two cycles* in $f$, of lengths $\ell_1$ and $\ell_2$ respectively, *into one cycle* of $\tau \circ f$ of length $\ell$ with

$$\ell = \ell_1 + \ell_2$$

Discussion 12.10 gives us the following lemma

**Lemma 12.11.** *Let $S$ be a finite set, and $f$ a permutation and $\tau$ a transposition of $S$. Then,*

$$\operatorname{sgn}(\tau \circ f) = -\operatorname{sgn}(f)$$

*Proof.* We use the cases we laid out in Discussion 12.10. In Case (1), we have

$$\operatorname{sgn}(\tau \circ f) = \operatorname{sgn}(\tau) \cdot \operatorname{sgn}(f) = -\operatorname{sgn}(f)$$

In Case (2), only the sign $(-1)^{\ell-1}$ in $f$ has been replaced with the following in $\tau \circ f$

$$(-1)^{\ell_1-1} \cdot (-1)^{\ell_2-1} = (-1)^{\ell_1+\ell_2-2} = (-1)^{\ell} = -(-1)^{\ell-1}$$

resulting in a change of sign.

In Case (3), only the sign $(-1)^{\ell_1-1} \cdot (-1)^{\ell_2-1}$ in $f$ has been replaced with the following in $\tau \circ f$

$$(-1)^{\ell_1+\ell_2-1} = -(-1)^{\ell_1+\ell_2-2} = -(-1)^{\ell_1-1} \cdot (-1)^{\ell_2-1}$$

resulting in a change of sign. □

**Theorem 12.12** (Characterisation 2 of Sign)**.** *Let $S$ be a finite set and $f$ a permutation of $S$.*

*If $f$ is written as a composition of $n$-many transpositions, then*

$$\operatorname{sgn}(f) = (-1)^n$$

*Proof Sketch.* Using Proposition 12.9, write

$$f = \tau_n \circ \tau_{n-1} \circ \cdots \circ \tau_1$$

where $\tau_i$'s are transpositions. Declare $h = \tau_{n-1} \circ \cdots \circ \tau_1$, giving you $f = \tau_n \circ h$ and therefore

$$\operatorname{sgn}(f) = \operatorname{sgn}(\tau_n \circ h) = -\operatorname{sgn}(h)$$

by Lemma 12.11. Since $h$ is a composition of $(n-1)$-many transpositions, the proof follows by the employment of the method of induction with the above being the inductive step. □

Theorem 12.12 allows us to give the following wondrous property of sign of a permutation.

**Corollary 12.13.** *Let $f$ and $g$ be permutations of a finite set $S$. Then,*

$$\operatorname{sgn}(g \circ f) = \operatorname{sgn}(g) \cdot \operatorname{sgn}(f)$$

*Proof.* Write

$$g = \tau_1 \circ \cdots \circ \tau_m \qquad \text{and} \qquad f = \tau'_1 \circ \cdots \circ \tau'_n$$

where $\tau_i$'s and $\tau'_j$'s are transpositions (using Proposition 12.9); so $\operatorname{sgn}(g) = (-1)^m$ and $\operatorname{sgn}(f) = (-1)^n$. Then,

$$g \circ f = \tau_1 \circ \cdots \circ \tau_n \circ \tau'_1 \circ \cdots \circ \tau'_m$$

is a composition of $(m+n)$-many transpositions. Therefore, $\operatorname{sgn}(g \circ f) = (-1)^{m+n}$ by Theorem 12.12. Thus,

$$\operatorname{sgn}(g \circ f) = (-1)^{m+n} = (-1)^m \cdot (-1)^n = \operatorname{sgn}(g) \cdot \operatorname{sgn}(f)$$ □

We will now works towards presenting a *third characterisation* of the sign of a permutation.

**Definition 12.14** (Inversions)**.** Let $S$ be a finite set of $\mathbb{Z}_+$ (or any finite set of $\mathbb{R}$) and let $f$ be a permutation of $S$.

An **inversion** of $f$ is an ordered pair $(i, j) \in S \times S$ such that

$$i < j \quad \text{and} \quad f(i) > f(j)$$

The **number of inversions** of $f$ is denoted $\operatorname{Inv}(f) \coloneqq \#\{(i, j) \in S \times S \,:\, i < j \text{ and } f(i) > f(j)\}$

**Example 12.15.**

- Consider the transposition $f = \tau_{1,3}$ on $S = \{1, 2, 3\}$. Then, $(1, 2)$, $(1, 3)$ and $(2, 3)$ are inversions since

  $$1 < 2 \quad \text{and} \quad f(1) = 3 > 2 = f(2)$$
  $$1 < 3 \quad \text{and} \quad f(1) = 3 > 1 = f(3)$$
  $$2 < 3 \quad \text{and} \quad f(2) = 2 > 1 = f(3)$$

  Therefore $\operatorname{Inv}(\tau_{1,3}) = 3$. While the transposition $\tau_{1,2}$ only has $(1, 2)$ as an inversion, and hence $\operatorname{Inv}(\tau_{1,2}) = 1$.

- Consider the following permutation on $S = \{1, 2, 3, 4, 5, 6\}$

  $$f = \begin{bmatrix} 1 & & 2 & & \\ \downarrow\uparrow & & \swarrow\nwarrow & & \circlearrowleft \\ 3 & & 4 \rightarrow 6 & & 5 \end{bmatrix}$$

  We build the following table populated with $(f(i), f(j))$ for $1 \leqslant i < j \leqslant 6$ to find its inversions.

| $i$ \ $j$ | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| 1 | $(3, 4)$ | $\boxed{(3, 1)}$ | $(3, 6)$ | $(3, 5)$ | $\boxed{(3, 2)}$ |
| 2 | | $\boxed{(4, 1)}$ | $(4, 6)$ | $(4, 5)$ | $\boxed{(4, 2)}$ |
| 3 | | | $(1, 6)$ | $(1, 5)$ | $(1, 2)$ |
| 4 | | | | $\boxed{(6, 5)}$ | $\boxed{(6, 2)}$ |
| 5 | | | | | $\boxed{(5, 2)}$ |

  Inversions of $f$ are $\boxed{\text{boxed}}$

  Therefore $\operatorname{Inv}(f) = 7$.

Our main goal is to prove the following:

**Theorem 12.16** (Characterisation 3 of Sign)**.** *Let $S$ be a finite set and $f$ a permutation of $S$. Then*

$$\operatorname{sgn}(f) = (-1)^{\operatorname{Inv}(f)} = \begin{cases} +1 & \text{if } f \text{ has even-many inversions} \\ -1 & \text{if } f \text{ has odd-many inversions} \end{cases}$$

**Definition 12.17** (Adjacent Transposition)**.** Let $S$ be a finite subset of $\mathbb{Z}_+$. A transposition of $S$ is called an **adjacent transposition** if it switches two *consecutive* numbers. In particular, it is a transposition of the form $\tau_{a,a+1}$.

**Lemma 12.18.** *Let $f$ be a permutation of $S = \{1, 2, \ldots, n\}$, where $n > 1$ is an integer, and $s = \tau_{a,a+1}$ be the adjacent transposition of $S$ swapping $a$ and $a+1$. Define*

$$u \coloneqq f^{-1}(a) \quad \text{so that} \quad f(u) = a \qquad\qquad v \coloneqq f^{-1}(a+1) \quad \text{so that} \quad f(v) = a+1$$

*Then we have*

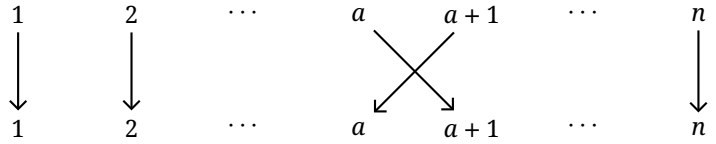
$$\operatorname{Inv}(s \circ f) = \begin{cases} \operatorname{Inv}(f) + 1 & \text{if } u < v \\ \operatorname{Inv}(f) - 1 & \text{if } u > v \end{cases}$$

*Proof.* Let $(i, j) \in S \times S$ such that $i < j$. Then $(i, j)$ is an inversion of $s \circ f$ if and only if

$$(s \circ f)(i) > (s \circ f)(j), \quad \text{which is equivalent to } \; s(f(i)) > s(f(j))$$

Recall that

$s$ is the permutation:




Consider the two-element set $\{f(i), f(j)\}$.

**Case (A)** If $\{f(i), f(j)\} = \{a, a+1\}$, then $s$ *does* invert the order relation between $f(i)$ and $f(j)$. Moreover, one obtains $\{f(i), f(j)\} = \{a, a+1\}$ exactly when $\{i, j\} = \{u, v\}$

**Case (A-1)** If $u < v$, then

$$s(f(u)) = s(a) = a+1 \qquad\qquad s(f(v)) = s(a+1) = a$$

Therefore $(u, v)$ is an inversion of $s \circ f$ but $(u, v)$ is not an inversion of $f$ since

$$f(u) = a < a+1 = f(v).$$

Hence $s \circ f$ has *one more inversion* than $f$ does when $u < v$.

**Case (A-2)** If $u > v$, then

$$s(f(u)) = s(a) = a+1 \qquad\qquad s(f(v)) = s(a+1) = a$$

Therefore $(u, v)$ is not an inversion of $s \circ f$ but $(u, v)$ is an an inversion of $f$ since

$$f(u) = a < a+1 = f(v).$$

Hence $s \circ f$ has *one less inversion* than $f$ does when $u > v$.

**Case (B)** If $\{f(i), f(j)\} \neq \{a, a+1\}$, then $s$ *does not* invert the order relation between $f(i)$ and $f(j)$. Thus, in this case, $(i, j)$ is an inversion of $s \circ f$ if and only if it is an inversion of $f$.

Thus, from Cases (A-1) and (B) we obtain

$$\mathsf{Inv}(s \circ f) = \mathsf{Inv}(f) + 1, \quad \text{if } u < v$$

and from Cases (A-2) and (B) we obtain

$$\mathsf{Inv}(s \circ f) = \mathsf{Inv}(f) - 1, \quad \text{if } u > v$$

as claimed. □

**Corollary 12.19.** *Any permutation $f$ of $S = \{1, 2, \ldots, n\}$ is a composite of $\mathsf{Inv}(f)$-many adjacent transpositions.*

*Proof.* We prove by inducting on $\mathsf{Inv}(f)$.

BASE CASE. Assume $\mathsf{Inv}(f) = 0$, then $f$ preserves order and therefore necessarily $f = \mathrm{id}_S$. Indeed $\mathrm{id}_S$ is a composition of 0-many (adjacent) transpositions.

Assuming the inductive hypothesis, consider a permutation $f$ with $\mathsf{Inv}(f) > 0$. Necessarily, $f \neq \mathrm{id}_S$ and therefore $f^{-1} \neq \mathrm{id}_S$. Hence, there must exist an $a \in S$ such that $f^{-1}(a) > f^{-1}(a+1)$.

Let $u = f^{-1}(a)$ and $v = f^{-1}(a+1)$. Thus, $f$ is a permutation of $f$ with $u > v$ and $f(u) = a < a+1 = f(v)$. Therefore, by Lemma 12.18

$$\mathsf{Inv}(\tau_{a,a+1} \circ f) = \mathsf{Inv}(f) - 1$$

Hence, we may apply the inductive hypothesis to $\tau_{a,a+1} \circ f$ concluding that $\tau_{a,a+1} \circ f$ is a composition of $(\mathsf{Inv}(f) - 1)$-many adjacent transpositions.

Finally, observe that

$$\begin{aligned} f &= \mathrm{id}_S \circ f \\ &= (\tau_{a,a+1} \circ \tau_{a,a+1}) \circ f \\ &= \tau_{a,a+1} \circ (\tau_{a,a+1} \circ f) \end{aligned} \tag{💬}$$

Since $\tau_{a,a+1}$ is an adjacent transposition and $\tau_{a,a+1} \circ f$ is a composition of $(\mathsf{Inv}(f) - 1)$-many adjacent transpositions, (💬) allows us to deduce that $f$ is a composition of $\mathsf{Inv}(f)$-many transposition.

Therefore we have proved our claim by the method of mathematical induction. □

*Proof of Theorem 12.16.* By Corollary 12.19 we may write any permutations $f$ as

$$f = s_1 \circ \cdots \circ s_{\mathsf{Inv}(f)}$$

where $s_i$'s are adjacent transpositions. In particular, $\mathsf{sgn}(s_i) = -1$. Therefore, by Corollary 12.13 we conclude

$$\mathsf{sgn}(f) = (-1)^{\mathsf{Inv}(f)}$$

as claimed. □

## 12.2. Permutations and Quadratic Reciprocity

Let $p$ be a fixed odd prime, and consider $\underline{\mathsf{R}}(p) = \{0, 1, \ldots, p-1\}$. For $b \in \mathbb{Z}$, consider the map

$$\mathbf{A}_b : \underline{\mathsf{R}}(p) \to \underline{\mathsf{R}}(p),\ x \mapsto [b + x]_p$$

where $[b + x]_p$ means taking the natural representative of $b + x$ modulo $p$.

**Lemma 12.20.** *The map $\mathbf{A}_b$, as a permutation of $\underline{\mathsf{R}}(p)$, has $\mathsf{sgn}(\mathbf{A}_b) = +1$.*

*Proof.* If $b \equiv 0 \bmod p$, then $\mathbf{A}_b = \mathrm{id}_{\underline{\mathsf{R}}(p)}$ and therefore has sign $= +1$.

If $b \not\equiv \bmod p$, then the (natural representatives of the) iterates

$$\{0,\ b,\ 2b,\ \ldots,\ (p-1)b\}$$

must be all of $\underline{\mathsf{R}}(p)$ since $b$ has a multiplicative inverse modulo $p$. That is, the cycle diagram of $\mathbf{A}_b$ has exactly one cycle of length $p-1$. Therefore, since $p$ is odd,

$$\mathsf{sgn}(\mathbf{A}_b) = (-1)^{p-1} = +1$$ □

**Lemma 12.21** (Zolotarev, 1872)**.** *For $\underline{\mathsf{U}}(p) = \{1, 2, \ldots, p-1\}$, consider the following for an integer $a \not\equiv 0 \bmod p$*

$$\mathbf{M}_a : \underline{\mathsf{U}}(p) \to \underline{\mathsf{U}}(p),\ x \mapsto [a \cdot x]_p$$

*$\mathbf{M}_a$, as a permutation of $\underline{\mathsf{U}}(p)$, has sign $\left(\frac{a}{p}\right)$.*

*Proof.* Recall the notation

$\ell(a)$ = the common length of the cycles in the dynamics of $\mathbf{M}_a$ in $\underline{\mathsf{U}}(p)$

$c(a)$ = the number of cycles

Moreover, $\ell(a) \cdot c(a) = p-1$, which is even since $p$ is odd. By definition of sign (Definition 12.5), we have

$$\mathsf{sgn}(\mathbf{M}_a) = ((-1)^{\ell(a)-1})^{c(a)} = (-1)^{\ell(a)\cdot c(a)} \cdot (-1)^{-c(a)} = (-1)^{p-1} \cdot (-1)^{c(a)} = (-1)^{c(a)}$$

since $p-1$ is even.

We consider two cases based on the parity of $c(a)$.

**Case (A)** Assume $c(a)$ is even, then $\mathsf{sgn}(\mathbf{M}_a) = +1$. On the other hand, since $a^{\ell(a)} \equiv 1 \bmod p$, we have

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = a^{\ell(a)\cdot\frac{c(a)}{2}} = (a^{\ell(a)})^{\frac{c(a)}{2}} \equiv 1^{\frac{c(a)}{2}} = 1 \bmod p$$

Therefore $\mathsf{sgn}(\mathbf{M}_a) = \left(\frac{a}{p}\right)$.

**Case (B)** Assume $c(a)$ is odd, then $\mathsf{sgn}(\mathbf{M}_a) = -1$. On the other hand, since $\ell(a)\cdot c(a) = p-1$ is even, necessarily $\ell(a)$ is even. Then $\ell(a)/2$ is an integer and

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

Since $\ell(a)$ is the smallest integer such that $a^{\ell(a)} \equiv 1 \bmod p$, we necessarily have

$$a^{\frac{\ell(a)}{2}} \not\equiv 1 \bmod p \quad \text{and hence} \quad a^{\frac{\ell(a)}{2}} \equiv -1 \bmod p$$

since $p$ is prime. We now have

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = a^{\frac{\ell(a)}{2}\cdot c(a)} = \left(a^{\frac{\ell(a)}{2}}\right)^{c(a)} \equiv (-1)^{c(a)} = -1 \bmod p$$

Therefore $\mathsf{sgn}(\mathbf{M}_a) = \left(\frac{a}{p}\right)$.

□

Reciprocity laws are deep by nature – their proofs never come easy. The proof we give below is no exception. It adapts an argument by Zolotarev, to uncover quadratic reciprocity in the signs of permutations.

We restate the theorem we wish to prove

**Theorem 12.22** (The Quadratic Reciprocity Law; Gauss)**.** *Let $p$ and $q$ be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}; \quad \textit{equivalently,} \quad \left(\frac{p}{q}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}\left(\frac{q}{p}\right)$$

*Proof.* We will consider a finite set of integers $X$ on which we will define three permutations $\alpha, \beta, \gamma$ such that

$$\operatorname{sgn}(\alpha) = \left(\frac{q}{p}\right), \qquad \operatorname{sgn}(\beta) = \left(\frac{p}{q}\right), \qquad \operatorname{sgn}(\gamma) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}, \qquad \text{and } \gamma \circ \alpha = \beta$$

Thereby giving us our result since then $\operatorname{sgn}(\gamma) \cdot \operatorname{sgn}(\alpha) = \operatorname{sgn}(\beta)$.

Let $X = \underline{\mathrm{R}}(pq) = \{0, 1, 2, \ldots, pq-1\}$.

The elements of $X$ can be described uniquely in three "bracket notations":

Let $a$ and $b$ be integers such that $0 \leqslant a \leqslant p-1$ and $0 \leqslant b \leqslant q-1$.

- Let $[a, b]$ be the unique element of $X$ congruent to $a \bmod p$ and $b \bmod q$.

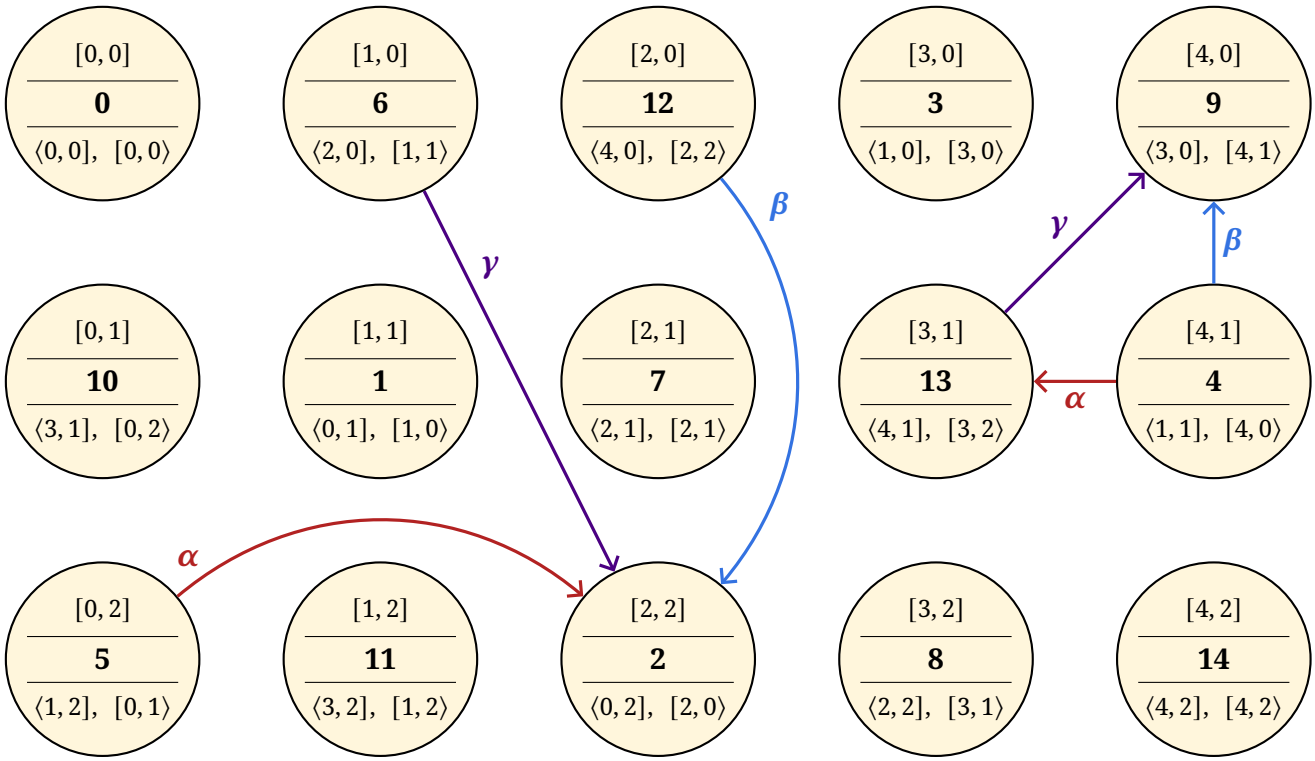
  This is the notation we used while discussing CRT.

- Let $\langle a, b]$, be the number $aq + b$.

- Let $[a, b\rangle$ be the number $a + bp$.

We visualise $X$ as a grid with $q$ rows and $p$ columns, where an element of $X$ labeled $[a, b]$ is placed at column $a$ and row $b$, with the other two bracket notations.

We visualise this for the case $p = 5$ and $q = 3$



On $X$ we define three permutations as follows:

- Let $\alpha$ be the permutation which sends the number labeled $[a, b]$ to that labeled $\langle a, b]$.
- Let $\beta$ be the permutation which sends the number labeled $[a, b]$ to that labeled $[a, b\rangle$.
- Let $\gamma$ be the permutation which sends the number labeled $\langle a, b]$ to that labeled $[a, b\rangle$.

We immediately see from the definition that

$$\gamma \circ \alpha = \beta$$

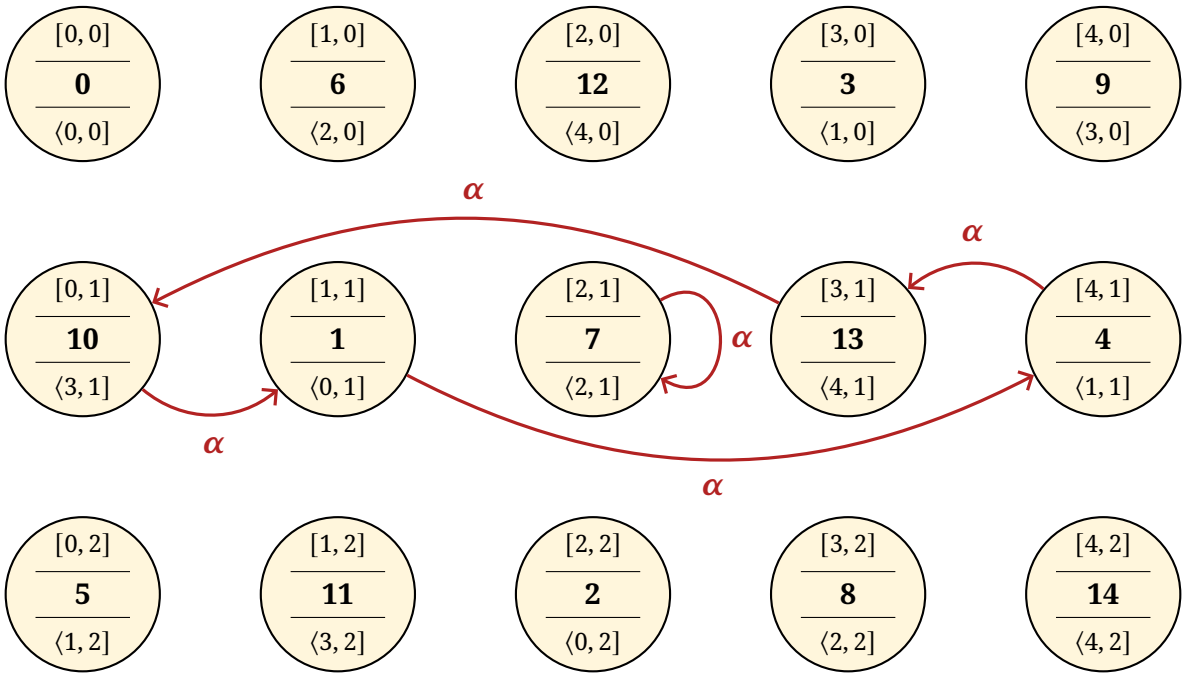
Our final task is to determine the signs of these permutations on $X$. We first prove that

$$\operatorname{sgn}(\alpha) = \left(\frac{q}{p}\right) \quad \text{and} \quad \operatorname{sgn}\beta = \left(\frac{p}{q}\right)$$

By symmetry it suffices to prove the statement for $\operatorname{sgn}(\alpha)$, since we obtain the statement for $\operatorname{sgn}(\beta)$ by swapping the roles of $p$ and $q$.

Let us investigate what $\alpha$ is doing to elements of $X$ as placed in a grid with $q$ rows and $p$ columns, where the number at column $a$ and row $b$ is the one labeled $[a, b]$. In particular, for $x \in X$ its row number is the natural representative of $x$ modulo $q$ and its column number is the natural representative of $x$ modulo $p$.

Consider $x = [a, b] \in X$ in column $a$ and row $b$. By definition, $\alpha(x) = \langle a, b] = aq + b$. Let us investigate the location of $\alpha(x)$ in the grid. Observe that $\alpha(x) = aq + b \equiv b \bmod q$ and therefore $\alpha(x)$ remains in row $b$. While $\alpha(x) = aq + b$ is in the column corresponding to the natural representative of $aq + b$ modulo $p$.




In summary, $\alpha$ does not change the rows of elements but it takes elements in column $a$ to elements in the column corresponding to the natural representative of $aq + b$ modulo $p$.

Within row $b$, $\alpha$ can then be interpreted as the permutation $\mathbf{A}_b \circ \mathbf{M}_q$ "multiply by $q$, then add $b$" modulo $p$ whose sign we can compute using Lemmas 12.20 and 12.21

$$\operatorname{sgn}(\mathbf{A}_b \circ \mathbf{M}_q) = \operatorname{sgn}(\mathbf{A}_b) \cdot \operatorname{sgn}(\mathbf{M}_q) = 1 \cdot \left(\frac{q}{p}\right) = \left(\frac{q}{p}\right)$$

The sign of $\alpha$ is the product of the signs obtained from each row, of which there are $q$ of them. Therefore

$$\mathsf{sgn}(\alpha) = \left(\frac{q}{p}\right)^q = \left(\frac{q}{p}\right)$$

since $q$ is odd and $(\pm 1)^q = \pm 1$. Thus, we have our claim.

We now prove that

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

where $\gamma$ sends the element in the grid labeled $\langle a, b]$ to the number labeled $[a, b\rangle$. That is, $\gamma\colon aq + b \mapsto a + bp$. We will compute its sign by counting the inversions of $\gamma$.

Consider $x, x' \in X = \{0, 1, 2, \ldots, pq - 1\}$. Dividing each of these by $q$ yields quotients $a, a'$ and remainders $b, b'$ respectively:

$$x = aq + b \quad \text{and} \quad x' = a'q + b'$$

Since $0 \leqslant b, b' \leqslant q - 1$, we see that

$$x < x' \quad \text{if and only if} \quad (a < a') \text{ or } (a = a' \text{ and } b < b') \tag{➔}$$

Now we compare $\gamma(x)$ and $\gamma(x')$ where we now have

$$\gamma(x) = a + bp \quad \text{and} \quad \gamma(x') = a' + b'p$$

Since $0 \leqslant a, a' \leqslant p - 1$, we see that

$$\gamma(x) > \gamma(x') \quad \text{if and only if} \quad (b > b') \text{ or } (b = b' \text{ and } a > a') \tag{➔}$$

An inversion occurs for $\gamma$ each time both (➔) and (➔) hold simultaneously. Eliminating some straightforward cases, we have

$$\boxed{x < x' \text{ and } \gamma(x) > \gamma(x')} \quad \text{if and only if} \quad \boxed{b > b' \text{ and } a < a'}$$

Thus, we must enumerate those $(a, a', b, b')$ where $0 \leqslant a < a' \leqslant p - 1$ and $0 \leqslant b' < b \leqslant q - 1$. This gives

$$\frac{p(p-1)}{2} \text{ possible pairs } (a, a') \qquad \text{and} \qquad \frac{q(q-1)}{2} \text{ possible pairs } (b, b')$$

which can be chosen independently. Therefore,

$$\mathsf{Inv}(\gamma) = \frac{p(p-1)}{2} \cdot \frac{q(q-1)}{2}$$

We compute

$$\mathsf{sgn}(\gamma) = (-1)^{\mathsf{Inv}(\gamma)} = (-1)^{\frac{p(p-1)}{2}\cdot\frac{q(q-1)}{2}} = ((-1)^{pq})^{\frac{(p-1)}{2}\cdot\frac{(q-1)}{2}} = (-1)^{\frac{(p-1)}{2}\cdot\frac{(q-1)}{2}}$$

since $p$ and $q$ are odd.

We conclude by observing that since $\gamma \circ \alpha = \beta$, we obtain

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

for distinct odd primes. □

**Remark 12.23.** There is a very fun way to visualise this argument we gave above – using playing cards! You can read more about this in these articles by Matt Baker and Jerry Shurman.

## Problems

**Problem 12.1. (challenge)** Zolotarev's lemma (Lemma 12.21) generalises to the Jacobi symbol (Problem 11.5).

Prove that for integers $n > 0$ and an element $u \in \underline{\mathsf{U}}(n)$

$$\mathbf{M}_u : \underline{\mathsf{R}}(n) \to \underline{\mathsf{R}}(n),\ y \mapsto [uy]_n$$

$\mathbf{M}_u$, as a permutation of $\underline{\mathsf{R}}(n)$, has sign $\left(\frac{a}{n}\right)$.

# 13. Proof of Quadratic Reciprocity à la Eisenstein following Gauss

In this section we provide a proof of Quadratic Reciprocity which is Eisenstein's simplification of a variation of Gauss's third proof of Quadratic Reciprocity.

The story begins with the following result of Gauss's that Gauss used to give his third proof in 1808.

**Lemma 13.1** (Gauss's Lemma, 1807)**.** *Let $p$ be an odd prime and let* $\gcd(a,p)=1$*. Let*

$$S=\left\{a,2a,\ldots,\left(\frac{p-1}{2}\right)a\right\} \quad \textit{and} \quad n=\#\left\{x\in S\ :\ [x]_p>\frac{p}{2}\right\}$$

*Then*

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

*Proof.* Let $n$ be as in the statement of the lemma, i.e. it is the number of elements in $S=\{ua\ :\ 1\leqslant k\leqslant (p-1)/2\}$ whose natural representatives modulo $p$ exceed $p/2$. Let us denote these natural representatives as

$$\{r_1,\ldots,r_n\}=\left\{[x]_p\ :\ x\in S \text{ and } \frac{p}{2}<[x]_p<p\right\}$$

Denote the natural representatives of the remaining elements of $S$ as

$$\{s_1,\ldots,s_m\}=\left\{[x]_p\ :\ x\in S \text{ and } 0<[x]_p<\frac{p}{2}\right\}$$

Necessarily, $n+m=(p-1)/2$ and $0<s_i,\ p-r_j<p/2$ for $1\leqslant i\leqslant m$ and $1\leqslant j\leqslant n$.

We will show that $s_i$'s are distinct from $p-r_j$'s. Assume to the contrary that $s_i=p-r_j$ for some $i$ and $j$. By definition, there exist integers $1\leqslant k,\ell\leqslant (p-1)/2$ such that

$$s_i\equiv ka \bmod p \quad \text{and} \quad r_j\equiv \ell a \bmod p$$

Then,

$$(k+\ell)a=ka+\ell a\equiv s_i+r_j=p\equiv 0 \bmod p$$

But observe that $1<k+\ell\leqslant p-1$ and $\gcd(a,p)=1$ by assumption and hence necessarily $(k+\ell)a\not\equiv 0 \bmod p$, contradicting our conclusion above. Thus, $s_i$'s are distinct from $p-r_j$'s.

Necessarily we deduce, since $0<s_i,\ p-r_j<p/2$, that

$$\left\{s_i,\ p-r_j\ :\ 1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n\right\}=\left\{1,2,\ldots,\frac{p-1}{2}\right\}$$

Therefore,

$$\begin{aligned}
\left(\frac{p-1}{2}\right)! &= s_1\cdot\ldots\cdot s_m\cdot(p-r_1)\cdot\ldots\cdot(p-r_n)\\
&\equiv s_1\cdot\ldots\cdot s_m\cdot(-r_1)\cdot\ldots\cdot(-r_n) \bmod p\\
&\equiv (-1)^n\cdot s_1\cdot\ldots\cdot s_m\cdot r_1\cdot\ldots\cdot r_n \bmod p\\
&\equiv (-1)^n\cdot a\cdot 2a\cdot\ldots\cdot\left(\frac{p-1}{2}\right)a \bmod p\\
&\equiv (-1)^n\cdot a^{\frac{p-1}{2}}\cdot 1\cdot 2\cdot\ldots\cdot\frac{p-1}{2} \bmod p\\
&\equiv (-1)^n\cdot a^{\frac{p-1}{2}}\cdot\left(\frac{p-1}{2}\right)! \bmod p
\end{aligned}$$

Since $\left(\frac{p-1}{2}\right)!$ is coprime to $p$, we may cancel the term to obtain

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

Using Euler's criterion (**??**), we conclude

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

as claimed. □

**Lemma 13.2** (Eisenstein's Lemma, 1844)**.** *If $p$ is an odd prime and $a$ is an odd integer with $\gcd(a, p) = 1$, then*

$$\left(\frac{a}{p}\right) = (-1)^{n_a}, \quad \textit{where } n_a = \sum_{u=1}^{p-1} \left\lfloor \frac{au}{p} \right\rfloor$$

*Proof.* As in Lemma 13.1, let $S = \{ua \ : \ 1 \leqslant u \leqslant (p-1)/2\}$ for an odd integer $a$ that is coprime to $p$. By the division algorithm, dividing $ua$ by $p$, we have

$$ua = pq_u + b_u$$

for $1 \leqslant u \leqslant (p-1)/2$ where $q_u$, $b_u$ are integers and $0 \leqslant b_u \leqslant p-1$. Therefore,

$$\frac{ua}{p} = q_u + \frac{b_u}{p}, \qquad \text{and hence} \quad \left\lfloor \frac{ua}{p} \right\rfloor = q_u$$

Therefore, we have

$$ua = \left\lfloor \frac{ua}{p} \right\rfloor p + b_u$$

If $b_u < p/2$, then necessarily it is one of the $s_i$'s from the proof of Lemma 13.1, and if $b_u > p/2$ then it is one of the $r_j$'s from the proof of Lemma 13.1. Therefore, we obtain

$$\sum_{u=1}^{\frac{p-1}{2}} ua = \sum_{u=1}^{\frac{p-1}{2}} \left\lfloor \frac{ua}{p} \right\rfloor p + \sum_{u=1}^{\frac{p-1}{2}} b_u = \sum_{u=1}^{\frac{p-1}{2}} \left\lfloor \frac{ua}{p} \right\rfloor p + \sum_{i=1}^{m} s_i + \sum_{j=1}^{n} r_j$$

Moreover, also recall from the proof of Lemma 13.1 that

$$\left\{s_i, \ p - r_j \ : \ 1 \leqslant i \leqslant m, \ 1 \leqslant j \leqslant n\right\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$$

and hence

$$\sum_{u=1}^{\frac{p-1}{2}} u = \sum_{i=1}^{m} s_i + \sum_{j=1}^{n} (p - r_j) = pn + \sum_{i=1}^{m} s_i - \sum_{j=1}^{n} r_j$$

Now observe the following

$$\begin{aligned}
(a-1) \sum_{u=1}^{\frac{p-1}{2}} u &= a \sum_{u=1}^{\frac{p-1}{2}} u - \sum_{u=1}^{\frac{p-1}{2}} u \\
&= \sum_{u=1}^{\frac{p-1}{2}} ua - \sum_{u=1}^{\frac{p-1}{2}} u \\
&= \left( \sum_{u=1}^{\frac{p-1}{2}} \left\lfloor \frac{ua}{p} \right\rfloor p + \sum_{i=1}^{m} s_i + \sum_{j=1}^{n} r_j \right) - \left( pn + \sum_{i=1}^{m} s_i - \sum_{j=1}^{n} r_j \right) \\
&= p \left( \sum_{u=1}^{\frac{p-1}{2}} \left\lfloor \frac{ua}{p} \right\rfloor - n \right) + 2 \sum_{j=1}^{n} r_j
\end{aligned}$$

Since $a$ and $p$ are odd by assumption, we have $a - 1 \equiv 0 \bmod 2$ and since $p \equiv 1 \bmod 2$. Therefore taking the above equation modulo 2 we obtain

$$n \equiv n_a = \sum_{u=1}^{\frac{p-1}{2}} \left\lfloor \frac{ua}{p} \right\rfloor \bmod 2$$

Therefore, by Lemma 13.1 we have

$$\left(\frac{a}{p}\right) = (-1)^n = (-1)^{n_a}$$

as claimed. □

We now give Eisenstein's proof of Quadratic Reciprocity from 1844.

**Theorem 13.3** (Quadratic Reciprocity Law)**.** *Let $p$ and $q$ be distinct odd primes. Then*

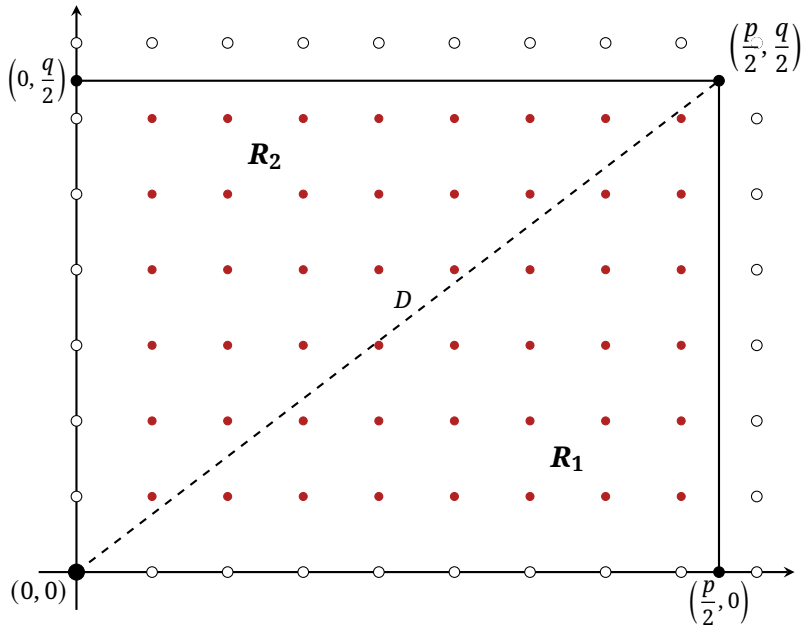
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

*Proof.* Let $p$ and $q$ be distinct odd primes. Consider the following rectangle with vertices $(0,0)$, $(p/2,0)$, $(0,q/2)$ and $(p/2,q/2)$. Let $R$ be the region within the rectangle excluding its boundary. We will be investigating *lattice points* in $R$, i.e., those points with integer coordinates.

Since $p$ and $q$ are odd, the lattice points $(k,\ell) \in \mathbb{Z}^2$ within $R$ are necessarily such that

$$1 \leqslant k \leqslant \frac{p-1}{2} \quad \text{and} \quad 1 \leqslant \ell \leqslant \frac{q-1}{2}$$

Therefore, the number of lattice points within $R$ is $\frac{p-1}{2} \cdot \frac{q-1}{2}$.




We will now count the lattice points in $R$ in a different way. Let $D$ be the diagonal of the rectangle – the line from $(0,0)$ to $(p/2,q/2)$. It divides $R$ into a lower triangle $R_1$ and an upper triangle $R_2$.

We first observe that $D$ is a line segment with the following equation

$$py = qx, \qquad \text{where } 0 \leqslant x \leqslant p/2,\ 0 \leqslant y \leqslant q/2$$

If there was a lattice point $(k, \ell)$ of $R$ on $D$ then $p\ell = qk$ where $0 < k < p/2$ and $0 < \ell < q/2$, which would necessarily give us $p \mid q$ or $q \mid p$ which is preposterous since $p$ and $q$ are distinct primes. Thus, no lattice points lie on $D$.

Therefore the lattice points of $R$ are either in $R_1$ or $R_2$. Let us start by counting lattice points in $R_1$.

Let $1 \leqslant u \leqslant (p-1)/2$ be an integer, and consider the vertical line $x = u$. It intersects $D$ at the point $\left(u, \dfrac{uq}{p}\right)$.

Therefore, the lattice points in $R_1$ lying on the line $x = u$ are those of the form $(u, v)$ where $v$ is an integer such that

$$0 < v < \frac{uq}{p} \quad \text{which is equivalent to} \quad 1 \leqslant v \leqslant \left\lfloor \frac{uq}{p} \right\rfloor$$

Therefore the number of lattice points on the line $x = u$ in $R_1$ is $\left\lfloor \dfrac{uq}{p} \right\rfloor$, and hence

$$\sum_{u=1}^{\frac{p-1}{2}} \left\lfloor \frac{uq}{p} \right\rfloor$$

is the total number of lattice points in $R_1$.

A symmetric argument for $R_2$, where we would consider the line $y = u$ instead, gives us that the total number of lattice points in $R_2$ are

$$\sum_{u=1}^{\frac{q-1}{2}} \left\lfloor \frac{up}{q} \right\rfloor$$

Thus, we have shown that

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{u=1}^{\frac{p-1}{2}} \left\lfloor \frac{uq}{p} \right\rfloor + \sum_{u=1}^{\frac{q-1}{2}} \left\lfloor \frac{up}{q} \right\rfloor = n_q + n_p$$

using notation from Lemma 13.2. Employing Lemma 13.2 gives us

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{n_q} \cdot (-1)^{n_p} = (-1)^{n_q + n_p} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

as we wished to prove. □

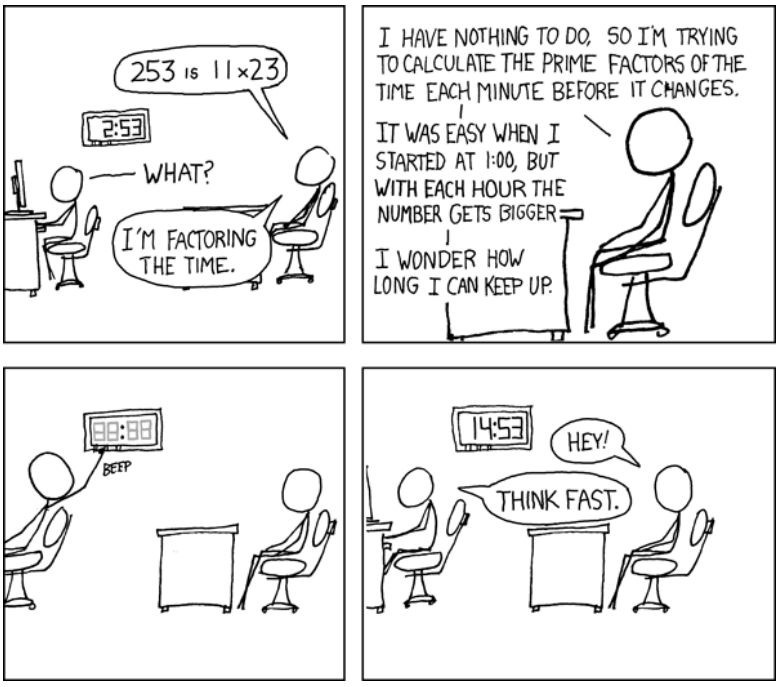
## References

[Wei17] Martin H. Weissman, *An Illustrated Theory of Numbers*, American Mathematical Society, Providence, RI, 2017.

---

*Mathematics is the queen of sciences and number theory is the queen of mathematics.*

– Carl Friedrich Gauss




FACTORING THE TIME – xkcd