LECTURE NOTES

MATH 110 — FALL 2021
INTRODUCTION TO NUMBER THEORY

University of California, Santa Cruz

DEEWANG BHAMIDIPATI

adapted from
Lectures by JUNECUE SUH
(MATH 110 — WINTER 2021)

Last Updated: Wednesday 16th March, 2022

Contents

1. Lecture 1 (9/23)

Numbers. For the purposes of this class, following number systems are the ones we care for:

- **Natural numbers**, $\mathbb{N} = \{0, 1, 2, \ldots\}$.

  Our natural numbers will include 0, and therefore will have a neutral element for both addition and multiplication.

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

  The "Z" comes from *Zahlen*, which is the German word for number.

  We will denote the set of positive integers as $\mathbb{Z}_+ = \{1, 2, 3, \ldots\}$.

- **Rational numbers**, $\mathbb{Q} = \left\{\frac{a}{b} \;:\; a, b \in \mathbb{Z},\, b \neq 0\right\}$.

  The "Q" stands for quotient.

- **Real numbers**, $\mathbb{R}$ are 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 π 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 "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 $\mathbb{Q}_p$.

- **Complex numbers**, $\mathbb{C} = \{a + bi \;:\; a, b \in \mathbb{R},\, i^2 = -1\}$.

  Complex numbers are an "algebraic jump" from the real numbers since i is a solution to the polynomial equation $x^2 + 1 = 0$.

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.

  ▷ On the application front, Elliptic Curve Cryptography is of this nature.

- **involving prime numbers**

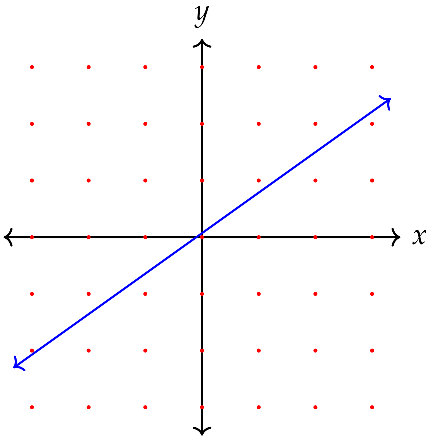
  ▷ counting prime numbers.
  A result of paramount importance here is the *Prime Number Theorem*.

  ▷ On the application front, the RSA cryptosystem is of this nature.

- **square a circle**: can there be a square whose area is π?
  Ans. No! This is related to the notion of transcendence and constructibility.

The (Euclidean) Division Algorithm

Linear Diophantine Equations. Let's pose a geometric question: in the euclidean plane, consider the integer grid and a line with rational slope and rational y-intercept



Does it intersect the integer grid?

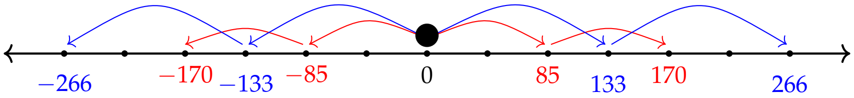
Algebraically, let $A, B, C \in \mathbb{Z}$, does there exist $(x, y) \in \mathbb{Z}^2$ such that

$$Ax + BY = C$$

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

Discussion. Visually, what we're asking for is this: suppose you are standing at 0 on the number line and you're allowed to

- *hop* 133 steps left (-133) or right (+133)
- *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*.

(Euclidean) Division Algorithm. The purpose is to check if $Ax + By = C$ has any integer solution and to find them all.

- Start with two positive integers a, b, assume $a \geqslant b$.
- Divide a by b
$$a = bq + r, \quad 0 \leqslant r < b, \quad q \in \mathbb{Z}$$
- 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.

Let's revisit the equation above, and see how the algorithm above makes it possible for us to find a required solution.

Example 1.1. *Employ the Division Algorithm to* $(133, 85)$ *and find a solution to the equation* $133x + 85y = 1$.

Answer. Let's employ the Division Algorithm

$$\begin{aligned}
133 &= 85 \cdot (1) + 48 \\
85 &= 48 \cdot (1) + 37 \\
48 &= 37 \cdot (1) + 11 \\
37 &= 11 \cdot (3) + 4 \\
11 &= 4 \cdot (2) + 3 \\
4 &= 3 \cdot (1) + 1 \\
3 &= 1 \cdot (3) + 0
\end{aligned}$$

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

$$\begin{aligned}
1 &= 4 + 3 \cdot (-1) \\
&= 4 + (11 - 4 \cdot (2)) \cdot (-1) \\
&= 11 \cdot (-1) + 4 \cdot (3) \\
&= 11 \cdot (-1) + (37 - 11 \cdot (3)) \cdot (3) \\
&= 37 \cdot (3) + 11 \cdot (-10) \\
&= 37 \cdot (3) + (48 - 37 \cdot (1)) \cdot (-10) \\
&= 48 \cdot (-10) + 37 \cdot (13) \\
&= 48 \cdot (-10) + (85 - 48 \cdot (1)) \cdot (13) \\
&= 85 \cdot (13) + 48 \cdot (-23) \\
&= 85 \cdot (13) + 133 - 85 \cdot (1) \cdot (-23) \\
&= 133 \cdot (-23) + 85 \cdot (36)
\end{aligned}$$

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

Example 1.2. *Does there exist a solution to the equation* $91x + 49y = 1$.

Answer. Let's 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's 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 $\text{GCD}(91, 49)$ and the last non-zero remainder we obtained using the division algorithm. This is not a coincidence.

Remark 1.3. 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 $(-23c, 36c)$.

Definition 1.4 (Greatest Common Divisor)**.** Let a, b be non-zero integers, than any positive integer g is called a *greatest common denominator* of a and b, denoted $\text{GCD}(a, b)$ or $\text{GCD}(b, a)$, if

(D1) $g \mid a$ and $g \mid b$, i.e. if g is a common divisor; and

(D2) d is any integer such that $d \mid a$ and $d \mid b$, then $d \mid g$.

e.g. $\text{GCD}(-4, 6) = 2$, $\text{GCD}(91, 49) = 7$, $\text{GCD}(133, 85) = 1$

Lemma 1.5. *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 1.1); thus, the GCD is unique. □

Theorem 1.6. *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* $\text{GCD}(a, b)$.

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

Lemma 1.7. *Let u, v, q, r be integers such that $u = vq + r$, then*

$$g = \mathrm{GCD}(u, v) \iff g = \mathrm{GCD}(v, r)$$

Proof. ($\Rightarrow$) Suppose $g = \mathrm{GCD}(u, v)$, let's prove $g = \mathrm{GCD}(v, r)$.

(i) Since $g = \mathrm{GCD}(u, v)$, therefore $g \mid u$ and $g \mid v$. Since $u = vq + r$, hence $r = u - vq$ and thus $g \mid r$ (see Problem 1.1). Therefore $g \mid v$ and $g \mid r$.

(ii) 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 $g = \mathrm{GCD}(u, v)$, by definition $g \mid d$.

By definition, we then have $g = \mathrm{GCD}(v, r)$. A very similar argument gives you ($\Leftarrow$). □

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

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

Our Lemma 1.7 tells us that

$$\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r_1) = \mathrm{GCD}(r_1, r_2) = \cdots = \mathrm{GCD}(r_{n-3}, r_{n-2}) = \mathrm{GCD}(r_{n-2}, R)$$

Note that in (Step n) we have obtained $R \mid r_{n-2}$ and therefore $\mathrm{GCD}(r_{n-2}, R) = R$ (see Problem 1.2). Hence $R = \mathrm{GCD}(a, b)$, as needed to be shown. □

Example 1.8 (in-class). *Consider the pair* $(39, 14)$, *using the Division Algorithm determine* $\mathrm{GCD}(39, 14)$ *and find a solution to* $39x + 14y = \mathrm{GCD}(39, 14)$.

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

Theorem 1.9 (Bézout's Identity). *Given non-zero integers a, b, there exist integers x, y such that*

$$ax + by = \mathrm{GCD}(a, b)$$

Proof. Consider $|a|, |b| > 0$, then by Theorem 1.6 and working the Division Algorithm backwards as in Example 1.1 we find integers x, y such that

$$|a|x + |b|y = \mathrm{GCD}(a, b)$$

- *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. □

1.1. Problems

Problem 1.1 (Divisibility)**.** Consider integers x, y, we say that x divides y, 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 1.2. Let a, b be non-zero integers. Prove that

(i) $\mathrm{GCD}(a, 0) = |a|$; $\mathrm{GCD}(a, 1) = 1$.

(ii) if $b \mid a$, then $\mathrm{GCD}(a, b) = b$.

(iii) $\mathrm{GCD}(a, a + 1) = 1$;

(iv) $\mathrm{GCD}(a, b) = \mathrm{GCD}(|a|, |b|)$.

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

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

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

Problem 1.3. Let a, b, c be integers, and let $g := \mathrm{GCD}(a, \mathrm{GCD}(b, c))$.

(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 $g = \mathrm{GCD}(b, \mathrm{GCD}(a, c)) = \mathrm{GCD}(c, \mathrm{GCD}(a, b))$

For this reason, we will write $\mathrm{GCD}(a, b, c) := \mathrm{GCD}(a, \mathrm{GCD}(b, c))$, and call it *the* greatest common divisor of a, b and c.

Problem 1.4. Using Problem 1.3 define $\mathrm{GCD}(a_1, \ldots, a_n)$ for integers $a_1, \ldots, a_n$, where $n \geqslant 4$.

2. Lecture 2 (9/28)

We are concerned with finding solutions to the equation

$$Ax + By = C \tag{$\bigstar$}$$

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

Theorem 2.1 (Existence of a Solution)**.** ($\bigstar$) *has a solution if and only if* $g := \mathrm{GCD}(A, B) \mid C$.

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

$$Ax + By = C.$$

Since $g = \mathrm{GCD}(A, B)$, 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 ($\bigstar$). □

Example 2.2. *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 1.6, $\mathrm{GCD}(27, 105) = 3$, 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 2.3 (Least Common Multiple)**.** Let a, b be non-zero integers, than any positive integer ℓ is called a *least common multiple* of a and b, denoted $\mathrm{LCM}(a, b)$ or $\mathrm{LCM}(b, a)$, if

(M1) $a \mid \ell$ and $b \mid \ell$, i.e. if ℓ is a common multiple; and

(M2) m is any integer such that $a \mid m$ and $b \mid m$, then $\ell \mid m$.

e.g. $\text{LCM}(-4, 6) = 12$, $\text{LCM}(91, 49) = 637$

Goal. We want to compute the set $\{(x,y) \in \mathbb{Z}^2 \ : \ Ax + By = C\}$ provided $\text{GCD}(A,B) \mid C$, because otherwise this set is empty.

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

$$Ax_0 + By_0 = C \tag{1}$$

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

$$Ax_1 + By_1 = C \tag{2}$$

Then (2) $-$ (1) gives us

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

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

Proposition 2.4. *Let $A, B \in \mathbb{Z}$, then*

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

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

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

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

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

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

thus proving (i).

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

$$m := Ax'' = B(-y''),$$

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

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

Therefore

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

hence (ii) is proved. □

Theorem 2.5 (Algorithm to Solve (★))**.**

- *Compute* GCD(A, B) *using the Division Algorithm.*
- *If* GCD$(A, B) \nmid C$*, there exists no solution.*
- *If* GCD$(A, B) \mid C$*, then let* $g = \mathrm{GCD}(A, B)$ *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*

$$\begin{cases} x = x_0 + n \cdot \dfrac{\mathrm{LCM}(A,B)}{A} \\[2ex] y = y_0 - n \cdot \dfrac{\mathrm{LCM}(A,B)}{B} \end{cases}$$

  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 2.4. 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 2.6. *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 2.2. Further, we can calculate the LCM as follows (we will prove this later)

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

Therefore, the general solution is

$$x = 108 + n \cdot \frac{945}{27} = 108 + 35n$$

$$y = -27 - n \cdot \frac{945}{105} = -27 - 9n$$

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

Example 2.7 (in-class). *Find all solutions to the equation* $117x + 42y = 33$.

Prime Factorisation

Definition 2.8. 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.

Lemma 2.9. *Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\mathrm{GCD}(a, b) = 1$ (that is, a and b are coprime), then $a \mid c$.*

Proof. Since $\mathrm{GCD}(a, b) = 1$, 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 2.10 (useful property 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 $g := \mathrm{GCD}(p, b)$. So, $g \mid p$ and therefore $g = 1$ or $g = p$. If $g = p$, then we have $g \mid b$, a contradiction; hence $g = 1$. Thus, by Lemma 2.9 we get $p \mid c$. □

Theorem 2.11 (Fundamental Theorem of Arithmetic AKA Unique Prime Factorisation).
Let n be any positive 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, for every prime p, we have $e_p = f_p$.*

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 that

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

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

Hence the existence statement holds true for $n = 1$ and $n = 2$. Assume that the existence statement is true for every positive integer $< n$. So, consider n itself; if n is prime itself, 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 our assumption, both a and b possess prime factorizations, 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's 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 contradiction, suppose that there exists a prime q such that $e_q \neq f_q$; let's assume, without loss of generality, that $e_q < f_q$. Define $d_q = f_q - e_q > 0$, and consider

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

Then note 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 2.12. *Let a, b be positive integers with the following prime factorisation*

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

Then

(i) $ab = 2^{e_2+f_2} \cdot 3^{e_3+f_3} \cdots p^{e_p+f_p} \cdots$.

(ii) $a \mid b$ if and only if $e_p \leqslant f_p$, for every prime p.

Proof. (i) is a direct result of power rules. Let's prove (ii).

($\Rightarrow$) Suppose $a \mid b$, then $b = ac$ for some positive integer c. Let $c = 2^{g_2} \cdot 3^{g_3} \cdots p^{g_p} \cdots$, then

$$b = ac = 2^{e_2+g_2} \cdot 3^{e_3+g_3} \cdots p^{e_p+g_p} \cdots$$

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

($\Leftarrow$) Suppose $e_p \leqslant f_p$, define $g_p := f_p - e_p \geqslant 0$ for every prime p. Let $c := 2^{g_2} \cdot 3^{g_3} \cdots p^{g_p} \cdots$, then by definition $b = ac$, and therefore $a \mid b$. □

2.1. Problems

Problem 2.1. Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\mathrm{GCD}(a, b) = d$, then prove that $a \mid dc$.

Problem 2.2. Let $a, b, c \in \mathbb{Z}$. Prove that $\mathrm{GCD}(a, b) = 1$ if and only if $\mathrm{GCD}(a^2, b^2) = 1$.

Problem 2.3. Let $a, b \in \mathbb{Z}$. Then prove that if $g = \mathrm{GCD}(a, b)$, then $\mathrm{GCD}\left(\frac{a}{g}, \frac{b}{g}\right) = 1$.

Problem 2.4.

(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 2.5. Look at Problem 1.3, write and prove the statements analogous for the LCM.

Problem 2.6.

(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 three free independent integer parameters m and n (not unlike the case of two variables where we have one independent integer parameter).

Problem 2.7. Let a, b and n be positive integers, and $a^n \mid b^n$, prove that $a \mid b$.

Problem 2.8. Recall that $n! = 1 \cdot 2 \cdots (n-1) \cdot n$. 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 there's no bound on the length of gaps between primes.

3. Lecture 3 (9/30)

Lemma 3.1. *With the notation as in Proposition 2.12, we have*

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

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

In particular, $ab = \mathrm{GCD}(a,b)\,\mathrm{LCM}(a,b)$.

Proof. Suppose we have proven that the GCD and LCM have the given prime factorisation, then since $e_p + f_p = \min(e_p, f_p) + \max(e_p, f_p)$, therefore $ab = \mathrm{GCD}(a,b)\,\mathrm{LCM}(a,b)$.

Write $g := \mathrm{GCD}(a,b) = 2^{h_2} \cdot 3^{h_3} \cdots p^{h_p}$. Since $g \mid a$ and $g \mid b$, therefore $h_p \leqslant e_p$ and $h_p \leqslant f_p$ and hence $h_p \leqslant \min(e_p, f_p)$.

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

Therefore $h_p = \min(e_p, f_p)$, and hence $\mathrm{GCD}(a,b) = 2^{\min(e_2,f_2)} \cdot 3^{\min(e_3,f_3)} \cdots p^{\min(e_p,f_p)} \cdots$. A similar argument gives us the result for LCM. □

Example 3.2. *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 Corollary 3.1, we have

$$\mathrm{GCD}(a,b) = 2^1 \cdot 3^2 \cdot 5^0 \cdot 7^0 = 18$$

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

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 2.12,

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

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

Example 3.3 (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?*

Another important consequence of unique prime factorisation of positive integers

Theorem 3.4. *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 positive integers u and v such that $u \mid a$ and $v \mid b$, and $w = uv$.

In short, there's a bijection

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

where (non-standard notation) $\mathscr{D}(n) := \{d \in \mathbb{Z}_+ \ : \ d \mid n\}$, i.e. the set of positive divisors of n.

Proof. (i) follows from Problem 1.1. Let's prove (ii): consider a positive divisor w of ab, where the prime factorisation of a and b is 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 $\mathrm{GCD}(a, b) = 1$, 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 2.12. 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 2.12, $u \mid a$ and $v \mid b$.

This proves surjectivity of Φ, injectivity follows from uniqueness of prime factorisation. □

Definition 3.5. For any positive integer n,

$$\sigma_0(n) := \#\mathscr{D}(n),$$

that is, the number of positive divisors of n.

e.g. $\sigma_0(6) = \#\{1, 2, 3, 6\} = 4$

Remark 3.6. $\sigma_0(n) = 1$ 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 3.7. *For coprime positive integers a, b, we have $\sigma_0(ab) = \sigma_0(a)\sigma_0(b)$.*

Proof. Recall the bijection Φ from Theorem 3.4, therefore the cardinalities of the domain and codomain of Φ are equal. The cardinality of the domain being $\sigma_0(a)\sigma_0(b)$ and that of the domain being $\sigma_0(ab)$. Hence $\sigma_0(ab) = \sigma_0(a)\sigma_0(b)$. □

Corollary 3.8. *For a positive integer n with prime factorisation given as $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, we have*

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

Proof. Let p be a prime, then note that $\mathscr{D}(p^e) = \{p^f \,:\, 0 \leqslant f \leqslant e\}$ for any integer $e \geqslant 0$, and therefore $\sigma_0(p^e) = e+1$. Now, consider n as in the statement, then applying Corollary 3.7 iteratively we have

$$\begin{aligned}\sigma_0(n) &= \sigma_0(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) \\ &= \sigma_0(p_1^{e_1})\,\sigma_0(p_2^{e_2}) \cdots \sigma_0(p_r^{e_r}).\end{aligned}$$

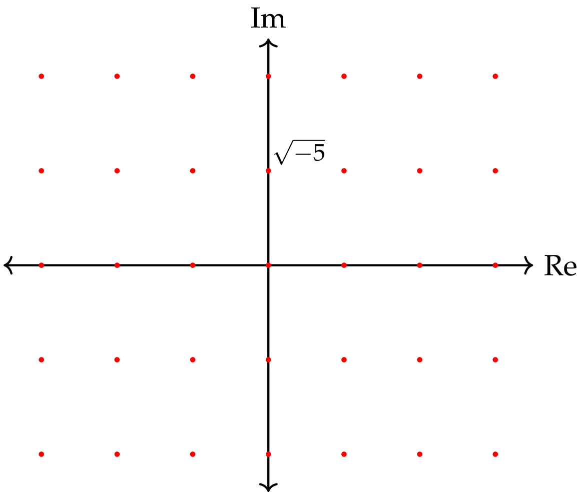
Then by our observations above, we get $\sigma_0(n) = (e_1+1)(e_2+1)\cdots(e_r+1)$. □

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

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

± 1 are called units.

Definition 3.9. $\mathcal{O} = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \,:\, a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$



Fact. $\mathcal{O}$ is closed under addition, subtraction and multiplication, and also contains 0 and 1. That is, $\mathcal{O}$ is a (commutative) ring.

Sketch of Fact. Let $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$ be elements of $\mathcal{O}$, then

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

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

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

$0 = 0 + 0\sqrt{-5}$ and $1 = 1 + 0\sqrt{-5}$. □

We'll mimic the definition of prime numbers in $\mathbb{Z}$ and introduce the notion of prime elements in the set $\mathcal{O}$.

Definition 3.10. A non-zero element α is called a *prime element* of $\mathcal{O}$ if

(P1) $\alpha \neq \pm 1$

(P2) for any $\beta, \gamma \in \mathcal{O}$ such that $\alpha = \beta\gamma$, then necessarily $\beta = \pm 1$ or $\gamma = \pm 1$

$\mathcal{O}$ does not admit a notion of *unique* prime factorisation, that is, elements in $\mathcal{O}$ can have two distinct prime factorisations. We illustrate this fact with an example, the content of which is Problem **??**; note

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

and we also know that there exists no $\gamma \in \mathcal{O}$ such that $2\gamma = 1 \pm \sqrt{-5}$.

3.1. Problems

Problem 3.1. Look at Problem 14, book. Let a, b be positive integers. Prove that $\mathrm{GCD}(a^k, b^k) = \mathrm{GCD}(a, b)^k$ and $\mathrm{LCM}(a^k, b^k) = \mathrm{LCM}(a, b)^k$ for any integer $k \geqslant 0$.

Problem 3.2. Let a, b and k be positive integers, then prove that $\mathrm{GCD}(ka, kb) = k \cdot \mathrm{GCD}(a, b)$ and $\mathrm{LCM}(ka, kb) = k \cdot \mathrm{LCM}(a, b)$.

Problem 3.3. Write the prime factorisation of $N = 13!$ and compute $\sigma_0(N)$.

Problem 3.4. As in class, consider the collection of complex numbers of the form:

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

(a) Consider the integer-valued function N defined on $\mathcal{O}$:

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

Prove that

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

for any two elements α and β in $\mathcal{O}$.

(b) Say that an element α in $\mathcal{O}$ is a **prime element** (prime elements are analogues of prime numbers) if

(i) $\alpha \neq 0, \pm 1$; and

(ii) whenever we have $\alpha = \gamma\delta$ with γ, δ in $\mathcal{O}$, we necessarily have $\gamma = \pm 1$ or $\delta = \pm 1$.

Prove that the following 4 elements are prime elements: 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$.

Hint: proceed by way of contradiction, then use part (a).

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

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

Problem 3.5. Let $T = \{1, 4, 7, 10, 13, 16, 19, \ldots\}$. 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 *nonunique* factorisation into irreducibles.

Problem 3.6. Prove that if n is a positive integer, and $\sigma_0(n)$ is prime then n is a power of a prime number.

Problem 3.7. What is the smallest positive integer with precisely 60 positive divisors?

4. Lecture 4 (10/5)

Distribution of prime numbers I. *Larger scale*

Theorem 4.1 (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 note 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 4.2. For any real number $x > 0$,

$$\pi(x) := \text{number of primes} \leqslant x$$

π is called the *prime counting function*.

e.g. $\pi(1.5) = 0, \pi(23) = \#\{2,3,5,7,11,13,17,19,23\} = 9.$

So, Euclid's theorem 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 4.3 (Prime Number Theorem, (1896) Hadamard, de la Vallée Poussin)**.**

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1,$$

where $\mathrm{Li}(x) = \displaystyle\int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$

Conjecture 4.4 (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 $\mathrm{li}(x) = \int_0^x \frac{dt}{\log t} = \mathrm{Li}(x) - \ln 2.$

Distribution of prime numbers I. *Smaller scale*

$$\underbrace{2,\ 3}_{1},\ 5,\ 7,\ 11,\ 13,\ \ldots,\ 263,\ 269,\ 271,\ 277,\ \ldots,$$

$$877,\ 881,\ 883,\ 887,\ 907,\ \ldots$$

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

Definition 4.5. *Twin primes* are a pair of primes (p, q) such that $|p - q| = 2$.

Conjecture 4.6. *There are infinitely many twin primes.*

Theorem 4.7. *There are infinitely many pairs (p, q) of primes such that*

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

Sum of Divisor functions.

Definition 4.8. A function $f : \mathbb{Z}_+ \to \mathbb{C}$ is called *multiplicative* if $f(ab) = f(a)f(b)$, for coprime positive integers a, b.

e.g. (1) Fix $k \in \mathbb{R}$, define $f_k(n) = n^k$. Then $f_k(ab) = (ab)^k = a^k b^k = f_k(a)f_k(b)$.

(2) Recall $\sigma_0 : \mathbb{Z}_+ \to \mathbb{C}$, where $\sigma_0(n)$ = number of positive divisors of n. Corollary 3.7 tells us that σ_0 is multiplicative.

Note that the coprime assumption is essential; consider, for instance, $a = 2$ and $b = 4$, then $\sigma_0(2 \cdot 4) = \sigma_0(8) = 4$. But $\sigma_0(2) = 2$ and $\sigma_0(4) = 3$, therefore $\sigma_0(2)\sigma_0(4) = 6 \neq 4 = \sigma_0(2 \cdot 4)$.

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

$$f(2 \cdot 3) = f(6) = 11$$

$$f(2) = 3; \quad f(3) = 5$$

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

Definition 4.9. Let $k \in \mathbb{R}$, define

$$\sigma_k : \mathbb{Z}_+ \to \mathbb{C}$$

as $\sigma_k(n) =$ sum of k-power of positive divisors of n, that is

$$\sigma_k(n) = \sum_{d \in \mathscr{D}(n)} d^k$$

Special Case. When $k = 0$, then $\sigma_0(n) = \sum_{d \in \mathscr{D}(n)} d^0 = \#\mathscr{D}(n) =$ number of positive divisors of n.

e.g. $k = 2$, $\sigma_2(6) = 1^2 + 2^2 + 3^2 + 6^2 = 50$.

Theorem 4.10. *For any $k \in \mathbb{R}$, σ_k is multiplicative.*

Proof. Let a, b be positive integers such that $\mathrm{GCD}(a, b) = 1$, then

$$\begin{aligned}
\sigma_k(ab) = \sum_{w \in \mathscr{D}(ab)} w^k &= \sum_{(u,v) \in \mathscr{D}(a) \times \mathscr{D}(b)} (uv)^k, \quad \text{by Theorem 3.4} \\
&= \sum_{u \in \mathscr{D}(a)} \sum_{v \in \mathscr{D}(a)} u^k v^k \\
&= \sum_{u \in \mathscr{D}(a)} u^k \left(\sum_{v \in \mathscr{D}(a)} v^k \right) \\
&= \sum_{u \in \mathscr{D}(a)} u^k \sigma_k(b) \\
&= \sigma_k(b) \left(\sum_{u \in \mathscr{D}(a)} u^k \right) = \sigma_k(b)\sigma_k(a)
\end{aligned}$$

Therefore $\sigma_k(ab) = \sigma_k(a)\sigma_k(b)$, whenever $\mathrm{GCD}(a, b) = 1$. □

We're now ready to introduce a strategy to compute $\sigma_k(n)$ for any given k and n, but first we review a proposition that we need.

Proposition 4.11. *Let $x \neq 1$ be a real number and e be a non-negative 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 4.12. *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 $d \in \mathscr{D}(p^e)$, we necessarily have $d = p^f$, $0 \leqslant f \leqslant e$ (in particular, $\sigma_0(p^e) = e + 1$). Therefore

$$\begin{aligned} \sigma_k(p^e) &= (p^0)^k + (p^1)^k + (p^2)^k + \cdots + (p^{e-1})^k + (p^e)^k \\ &= 1 + p^k + (p^k)^2 + \cdots + (p^k)^e \\ &= \frac{(p^k)^{e+1} - 1}{p^k - 1}, \quad \text{taking } x = p^e \text{ in Proposition 4.11} \end{aligned}$$

since $k \neq 0$. □

Example 4.13. *Compute $\sigma_3(12)$.*

Answer. First note that $12 = 2^2 \cdot 3$. Since $\text{GCD}(2^2, 3) = 1$, 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 $\sigma_3(12) = 2044$. □

So our general strategy to compute $\sigma_k(n)$, when $k > 0$, is as follows:

- Consider the prime factorisation of n, say $n = p_1^{e_1} \cdots p_r^{e_r}$
- Since $\text{GCD}(p_i, p_j) = 1$, therefore $\text{GCD}(p_i^{e_i}, p_j^{e_j}) = 1$ for $i \neq j$ (see Problem 1.2).
- Hence $\sigma_k(n) = \sigma_k(p_1^{e_1}) \cdots \sigma_k(p_r^{e_r})$.
- Apply Corollary 4.12 to $\sigma_k(p_i^{e_i})$.

One reason why we care about σ_k

Definition 4.14. Let n be a positive integer

(1) Say n is *perfect* if the sum of proper divisors of n, that is divisors strictly less than n, equals n. Equivalently, if $\sigma_1(n) = 2n$.

(2) Say n is *deficient* if $\sigma_1(n) < 2n$.

(3) Say n is *abundant* if $\sigma_1(n) > 2n$.

e.g. (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 24 is abundant.

Known perfect numbers: 6, 28, 496, 8128, 33550336, ... (about fifty).

Open Questions.

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

Example 4.15 (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?*

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

Proposition 4.16. *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

$$\begin{aligned} 2^n - 1 &= 2^{ab} - 1 \\ &= (2^a)^b - 1^b \\ &= (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1) \end{aligned}$$

These are non-unit proper divisors of $2^{ab} - 1$, since $1 < a, b < n$. Therefore this number is composite, giving us a contradiction. Hence n is prime. □

The converse is not true, that is, if n is prime then $2^n - 1$ is not necessarily prime.

e.g. $2^{11} - 1 = 2047 = 23 \cdot 89$.

4.1. Problems

Problem 4.1. For this problem, you may want to review one-variable Calculus.

(a) Recall the definition

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} \quad \text{for } x > 2$$

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

(b) Prove that

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

Problem 4.2. Compute $\sigma_1(N)$ for the three numbers $N = 28,\ N = 111$, and $N = 240$. Classify N as abundant, deficient or perfect.

Problem 4.3 (Mersenne, 1644)**.** Describe all circumstances under which $\sigma_1(n)$ is odd.

Problem 4.4. Find a short formula for $\sigma_0(p) + \sigma_1(p) + \cdots + \sigma_k(p)$ whenever p is a prime number.

Problem 4.5. 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 4.6. Prove that if n is a perfect square, then n is not a perfect number.

Problem 4.7. We say that a positive integer n is *square-free* if n is not divisible by p^2 for any prime number p. Necessarily, n is then a distinct product of primes. (E.g. 15 and 37 are square-free, but 24 and 49 are not.)

Consider the function μ (named after A.F. Möbius, popularly known for his strip) defined on positive integers n as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \text{ is not square-free} \\ (-1)^t & \text{if } n \text{ is square-free and has exactly } t \text{ prime divisors.} \end{cases}$$

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

(b) Prove that μ 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 μ.

(c) Let $n > 1$ be any integer greater than 1. 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.

Problem 4.8. Let $f(n)$ and $g(n)$ be two complex-valued multiplicative functions of positive integers n. Define $h(n)$ by the formula:

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

(a) Consider the case where $g(n) = \mu(n)$ defined in Problem 4.7 above and $f(n) = n$. Compute the values of $h(n)$ for $n = 1, \ldots, 12$.

(b) Prove, in the general case of multiplicative functions f and g, that h is a multiplicative function.

(The new function h is called the *convolution* of f and g, and is denoted by $f \star g$. The idea originates from Fourier analysis.)

5. Lecture 5 (10/7)

We relate perfect numbers with certain kinds of prime numbers.

Definition 5.1. A *Mersenne prime* is a prime number M_p of the form $2^p - 1$ for some prime p.

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

Theorem 5.2 (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.*

e.g. $M_2 = 3,\ N_2 = 6;\ M_3 = 7,\ N_3 = 28;\ M_5 = 31,\ N_5 = 496.$

Proof. Recall that $\sigma_1(n) = \sum_{d \in \mathscr{D}(n)} d$, and that n is a perfect number if and only if $\sigma_1(n) = 2n$. Furthermore, since M_p is an odd prime, necessarily $\mathrm{GCD}(2^{p-1}, M_p) = 1$. Consider

$$\begin{aligned}
\sigma_1(N_p) &= \sigma_1(2^{p-1}M_p) \\
&= \sigma_1(2^{p-1}) \cdot \sigma_1(M_p), \quad \text{since } \mathrm{GCD}(2^{p-1}, M_p) = 1 \text{ and } \sigma_1 \text{ is multiplicative} \\
&= \frac{2^{p-1+1} - 1}{2 - 1} \cdot (1 + M_p) \\
&= 2^p(2^p - 1) \\
&= 2 \cdot 2^{p-1}M_p \\
&= 2N_p
\end{aligned}$$

Therefore N_p is an even perfect number. □

Theorem 5.3 (Euler, 1849)**.** *Suppose N is an even perfect number, then there exists a prime number p such that $N = N_p$, as in Theorem 5.2.*

Proof. Let N have the following prime factorisation

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

where $e_p \geqslant 0$ (and $e_p = 0$ for all $p > N$). Let $p := e_2 + 1$ and $q := N/2^{e_2} = 3^{e_3} \cdots p^{e_p} \cdots$. In particular, $N = 2^{p-1}q$.

Note that $\mathrm{GCD}(2^{p-1}, q) = 1$ since $2 \nmid q$. Since N is perfect, we have

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

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. Hence, $\sigma_1(q) = q + d$.

- *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 arrived at a contradiction again.

Hence q is prime, and thus necessarily $d = 1$, since it's a proper divisor of q. That is, $q = 2^p - 1$ is a prime, and so p is prime by Proposition 4.16. Thus, $q = M_p$ is a Mersenne prime and $N = N_p$. □

Rational Numbers

Definition 5.4. A *rational number* is a number of the form $\frac{a}{b}$, where a, b are integers and $b \neq 0$. A *fraction* is an expression of the form $\frac{a}{b}$, where a, b are integers and $b \neq 0$.

e.g. $\frac{2}{3}$ and $\frac{4}{6}$ are distinct fractions but equal as rational numbers.

Definition 5.5. Say a fraction $\frac{a}{b}$ is *reduced* if $\mathrm{GCD}(a, b) = 1$ and $b > 0$.

e.g. $\frac{2}{3}$ is reduced but $\frac{4}{6}$ isn't. $\frac{2}{-3}$ isn't reduced but $\frac{-2}{3} = -\frac{2}{3}$ is.

Theorem 5.6. *Let $\frac{a}{b}$ be a fraction, then there exists a unique fraction $\frac{c}{d}$ such that $\frac{a}{b} = \frac{c}{d}$ as rational numbers.*

e.g. $-1.56 = \dfrac{156}{-100} = \dfrac{39}{-25} = -\dfrac{39}{25}$

Proposition 5.7. *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) $x = \pm 2^{e_2} \cdot 3^{e_3} \cdots p^{e_p} \cdots$.

Proof (sketch). Write $x = \dfrac{a}{b}$ 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 $e_p := f_p - g_p$ gives us $x = \pm 2^{e_2} \cdot 3^{e_3} \cdots p^{e_p} \cdots$. □

e.g. $-1.56 = -\dfrac{39}{25} = -\dfrac{3 \cdot 13}{5^2} = -2^0 \cdot 3^1 \cdot 5^{-2} \cdot 7^0 \cdot 11^0 \cdot 13^1$

Definition 5.8. A complex number is *irrational* if it's not rational

e.g. $\sqrt{2}$ is irrational.

More generally,

Proposition 5.9. *Let a/b be a reduced fraction and let $n \geqslant 2$ be an integer. Then $\alpha = \sqrt[n]{a/b}$ if and only if a and b are n^{th} powers.*

Proof. ($\Rightarrow$) Suppose α is rational, so write $\alpha = c/d$ in reduced form, that is $\text{GCD}(c, d) = 1$ and $d > 0$. Then

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

Since $\text{GCD}(c, d) = 1$, therefore $\text{GCD}(c^n, d^n) = \text{GCD}(c, d)^n = 1$ by Problem 3.1 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 5.6 we get $a = c^n$ and $b = d^n$.

($\Leftarrow$) If a and b are n^{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 α is rational. □

e.g. (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.

Definition 5.10. Say a complex number α is *algebraic* if it's a root of a nonzero polynomial $P(T) = c_d T^d + \cdots + c_1 T + c_0$, where $c_i \in \mathbb{Z}$ with at least one of them being nonzero. That is, $P(\alpha) = c_d \alpha^d + \cdots + c_1 \alpha + c_0 = 0$.

Otherwise, that is if α is not algebraic, then say α is *transcendental*.

e.g. (0) Rational numbers are algebraic: let $\alpha = a/b$, then α is a root of $P(T) = bT - a$.

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

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

(3) $2\sqrt{2}+\sqrt{3}$ is algebra. Let's show this.

Fact. If α and β are algebraic, then

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

are all also algebraic.

(3) *continued*. 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 α is algebraic.

5.1. Problems

Problem 5.1. Prove Theorem 5.6.

Problem 5.2.

(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: what is the inverse of $\sqrt{2}-c$?

(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 5.3. 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

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

Prove that R_n is countable. Why is R_n infinite?

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

6. Lecture 6 (10/12)

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

Theorem 6.1 (Rational Root Theorem). *Let a/b be a rational number in reduced form such that it's 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

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

Therefore,

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

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

Therefore $b \mid c_d a^d$ and $a \mid c_0 b^d$. Since $\mathrm{GCD}(a,b) = 1$, hence $\mathrm{GCD}(a,b^d) = \mathrm{GCD}(a^d,b) = 1$. Thus $b \mid c_d$ and $a \mid c_0$, by Lemme 2.9. □

e.g. For $\alpha = 2\sqrt{2} + \sqrt{3}$, 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 $b \mid 1$. Therefore $a/b \in \{\pm 1, \pm 5, \pm 25\}$ but none of them equal $2\sqrt{2} + \sqrt{3}$.

Example 6.2 (in-class). *$\sqrt{3} + \sqrt{5}$ is algebraic and irrational.*

Examples of transcendental number. Note that $\mathbb{C}$ is uncountable but the set of all algebraic numbers is countable. Therefore there are uncountably many transcendental numbers.

Theorem 6.3 (Lindemann & Weierstrass, 1800's). *π and e are transcendental.*

(But we don't yet know if $e + \pi$ is transcendental, for example.)

Corollary 6.4 (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 π.*

Other suspects. Let $k \geqslant 1$ be an integer, then

$$\zeta_k = 1 + \frac{1}{2^k} + \frac{1}{3^k} + \frac{1}{4^k} + \cdots$$

converges when $k > 1$.

Facts. (1) $\zeta_2 = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ (Basel problem, solved by Euler in 1734). ζ_2 is transcendental.

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

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

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

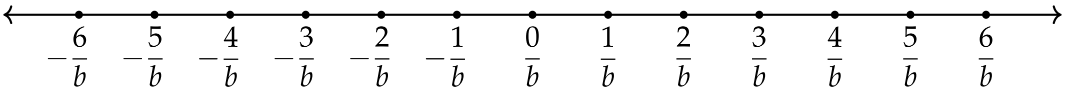
Open: is γ rational?

Diophantine Approximation. 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 $|x - q| < \varepsilon$.

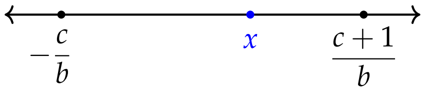
Proposition 6.5. *Let α be any real number and b a positive integer. Then there exists an integer a such that*

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

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. So,

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

□

Sometimes, we have a far better deal

e.g. $\pi = 3.1415926$

- $a/b = 3.14 = 314/100 = 157/100$; $|\pi - a/b| \approx 0.00159$. Compared to $1/2b = 1/100 = 0.01$, it's $\sim$ 16% off.
- $a/b = 22/7 = 3.\overline{142857}$; $|\pi - a/b| \approx 0.0013$. Compared to $1/2b = 1/14 = 0.07$, it's only $\sim$ 2% off.

Why do we care about this? To prove transcendence of numbers. For example, if we want to prove π or e is transcendental, then we 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 you can approximate an irrational number α by rational (or algebraic) numbers very well, then α is likely to be transcendental.

e.g. $e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots$. So,

$$e = x + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \cdots$$

Terms in the series decrease very rapidly, since $n!$ increases rapidly as $n \to \infty$.

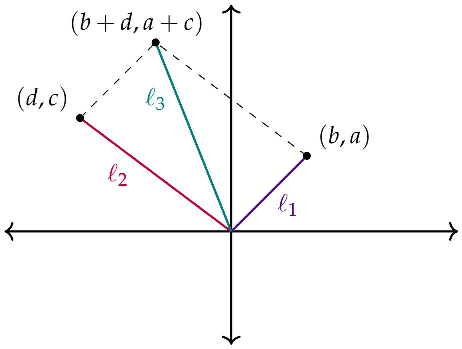
Definition 6.6. Let a/b and c/d be (reduced) fractions. The *mediant* of a/b and c/d is

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

e.g. $\frac{5}{3} \vee \frac{11}{17} = \frac{5+11}{3+17} = \frac{16}{20}$.

Proposition 6.7. *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 we get



Then note that

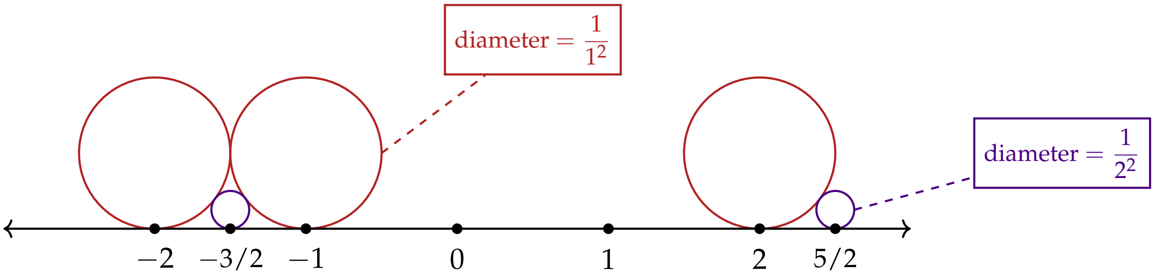
$$\frac{a}{b} \text{ is the slope of } \ell_1$$

$$\frac{c}{d} \text{ is the slope of } \ell_2$$

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

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 6.8. Let a/b be a reduced fraction; in particular $b > 0$. The *Ford circle atop* a/b is the circle of diameter $1/b^2$ that is above and tangent to the real line at the rational number a/b.



Note that some Ford circles are tangent to each other.

6.1. Problems

Problem 6.1.

(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 6.2. Consider the *Fibonacci numbers*[1], 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 are

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \dots.$$

(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 (to a real number).

(c) Prove that r_n converges to the *golden ratio*:

$$\phi = \frac{1+\sqrt{5}}{2}$$

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

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

Problem 6.3. 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 $s_n := \sum_{k=0}^{n} \frac{1}{k!}$, the n^{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 6.4. Using Problem 4.5, prove that for all positive integers n, we have

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

where γ is the Euler-Mascheroni constant.

7. Lecture 7 (10/14)

Definition 7.1. Let a/b and c/d be reduced fractions that are distinct as rational numbers. Then we say *a/b kisses c/d* if $ad - bc = \pm 1$. Notationally

$$\frac{a}{b} \heartsuit \frac{c}{d} \qquad \text{if and only if} \quad \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1$$

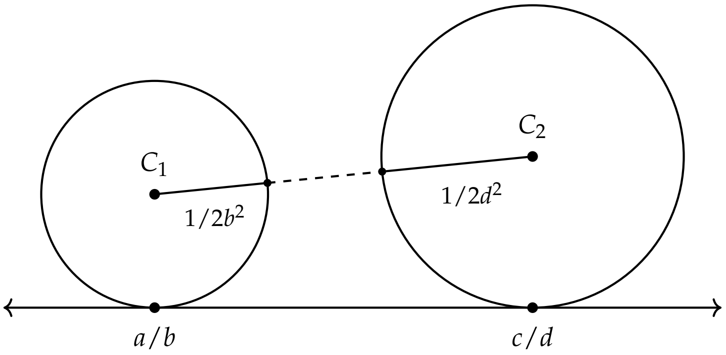
Proposition 7.2. *If a/b kisses any fraction c/d at all, then* $\mathrm{GCD}(a, b) = 1$.

Proof. By assumption, $ax + by = \pm 1$ has an integer solution: $(d, -c)$. Therefore $\mathrm{GCD}(a, b) \mid \pm 1$ and hence $\mathrm{GCD}(a, b) = 1$, necessarily. □

Theorem 7.3. *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. Let's set things up by first considering the Ford circles, say



where C_1 and C_2 are the centres of the Ford circles atop a/b and c/d respectively.

$$\text{Cartesian coordinates of } C_1 = \left(\frac{a}{b}, \frac{1}{2b^2}\right)$$

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

By Pythagoras' theorem (equivalently the distance formula)

$$\begin{aligned} \overline{C_1C_2}^2 &= \left(\frac{1}{2b^2} - \frac{1}{2d^2}\right)^2 + \left(\frac{a}{b} - \frac{c}{d}\right)^2 \\ &= \left(\frac{ad - bc}{bd}\right)^2 + \left(\frac{1}{2b^2} - \frac{1}{2d^2}\right)^2 \qquad (1) \end{aligned}$$

The Ford circles are tangent to each other if and only if

$$\begin{aligned} \overline{C_1C_2} &= \frac{1}{2b^2} + \frac{1}{2d^2} \\ \iff \overline{C_1C_2}^2 &= \left(\frac{1}{2b^2} + \frac{1}{2d^2}\right)^2 \\ \underset{(1)}{\iff} \left(\frac{ad-bc}{bd}\right)^2 + \left(\frac{1}{2b^2} - \frac{1}{2d^2}\right)^2 &= \left(\frac{1}{2b^2} + \frac{1}{2d^2}\right)^2 \\ \iff \left(\frac{ad-bc}{bd}\right)^2 &= \left(\frac{1}{2b^2} + \frac{1}{2d^2}\right)^2 - \left(\frac{1}{2b^2} - \frac{1}{2d^2}\right)^2 \\ \iff \left(\frac{ad-bc}{bd}\right)^2 &= 4\left(\frac{1}{2b^2}\right)\left(\frac{1}{2d^2}\right) \\ \iff (ad-bc)^2 &= 1 \\ \iff ad-bc &= \pm 1 \end{aligned}$$

if and only if $\frac{a}{b} \heartsuit \frac{c}{d}$. □

Proposition 7.4. *Let a/b be a reduced fraction. Then*

(1) a/b kisses infinitely many fractions.

(2) If $b > 1$, then there are exactly two reduced fractions c/d and c'/d', with $d, d' < b$, that kiss a/b such that $c/d \vee c'/d' = a/b$ and $c/d \heartsuit c'/d'$.

Proof.

(1) By assumption, $\text{GCD}(a,b) = 1$. So, if u/v is a reduced fraction kissing a/b, then by definition, $(x,y) = (v,u)$ is a solution to the equation

$$ax - by = \pm 1$$

We can take, without loss of generality, the equation $ax - by = 1$. Since $\text{GCD}(a,b) = 1 = ax + (-b)y$, by Theorem 2.5, all solutions to this equation are of the form

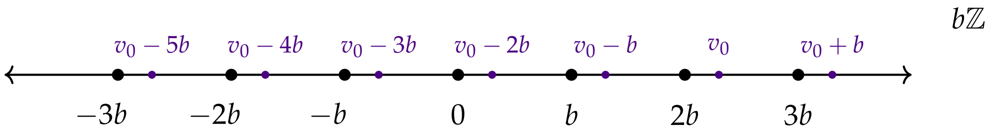
$$u_n = u_0 + an, \quad v_n = v_0 + bn \qquad (\text{since LCM}(a,-b) = -ab)$$

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

There's at most one n such that $v_n = 0$ since $b > 0$. Whenever $v_n \neq 0$, u_n/v_n or $-u_n/-v_n$ is a reduced fraction that kisses a/b.

Hence, there are infinitely many u/v's that kiss a/b. □

(2) We have $b > 1$; let's plot the values of $\{v_0 + bn\}_{n \in \mathbb{Z}}$, say



Where could v_0 lie? We cannot have $v_0 = nb$ for any $n \in \mathbb{Z}$, since the fact $av_0 - bu_0 = 1$ gives us $b = (an - u_0) = a(nb) - bu_0 = 1$, that is, $b \mid 1$. This is isn't possible as $b > 1$. Hence $v_0 \in (kb, (k+1)b)$ for some integer k.

Therefore, among $\{v_0 + bn\}_{n \in \mathbb{Z}}$, *exactly one* falls in $(0, b)$ and *exactly one* falls in $(-b, 0)$. Let $v_m \in \{v_0 + bn\}_{n \in \mathbb{Z}}$ be the one in $(0, b)$; we can then also consider u_m.

Then $u_m/v_m \heartsuit a/b$ and $0 < v_m < b$, so define $c/d := u_m/v_m$. Furthermore, also define $c'/d' := (a - u_m)/(b - v_m)$, then $d' < b$ and

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

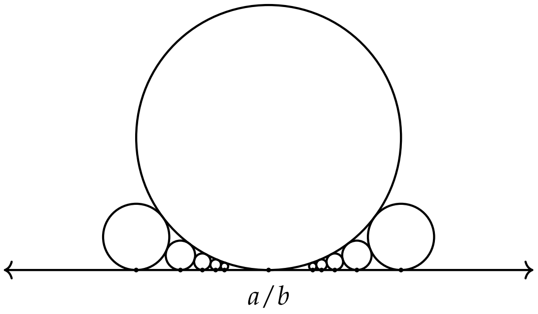
by constriction. Lastly, note that

$$\begin{aligned} cd' - c'd &= u_m(b - v_m) - (a - u_m)v_m \\ &= (bu_m - av_m) + (u_m v_m - u_m v_m) \\ &= -1 \end{aligned}$$

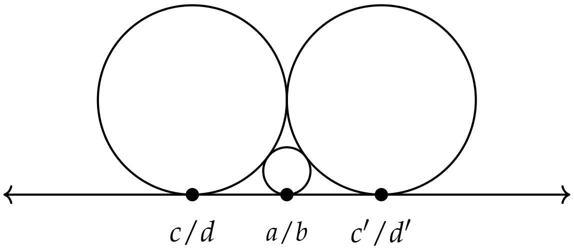
Thus, $c/d \heartsuit c'/d'$. □

Corollary 7.5 (geometric form)**.** *Let a/b be a reduced fraction. Then*

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



(2) 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 7.6. *Find the two kissing (reduced) fractions whose mediant is* $83/71$*.*

Answer. If x/y was one of them, then $71x - 83y = \pm 1$. Let's employ the division algorithm

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

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

Take $\frac{c}{d} = \frac{7}{6}$, note $6 < 71$, and $\frac{c'}{d'} = \frac{83-7}{71-6} = \frac{76}{65}$. □

Example 7.7 (in-class)**.** *Find the two kissing (reduced) fractions* a/b *and* c/d *whose mediant is* $15/32$*.*

Theorem 7.8. *Consider the following process*

- Step I. *Start with fractions* $\frac{n}{1}$ *as* n *runs through the integers.*
- Step II. *Whenever you see two kissing fractions, form their mediant.*
- Step III. *Keep repeating* Step II*.*

Then

(1) The fractions occurring in this sequence are reduced.

(2) 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.

(1) For $b = 1$, $a/1$ is reduced.

Assume the inductive hypothesis; if $\frac{a}{b} \heartsuit \frac{c}{d}$, we form $\frac{a}{b} \vee \frac{c}{d} = \frac{a+c}{b+d}$.

> **Lemma 7.9.** *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 $\left(\frac{x}{y} \vee \frac{z}{w}\right) \heartsuit \frac{x}{y}$. □

Now, since $\left(\frac{a}{b} \vee \frac{c}{d}\right) \heartsuit \frac{a}{b}$, the mediant is reduced by Proposition 7.2. □

(2) If $b = 1$, then $\frac{a}{1}$ occurs in the base step.

Assume the inductive hypothesis; now $b > 1$, therefore by Proposition 7.4 there exist reduced fractions c/d and c'/d' with $d, d' < b$ such that

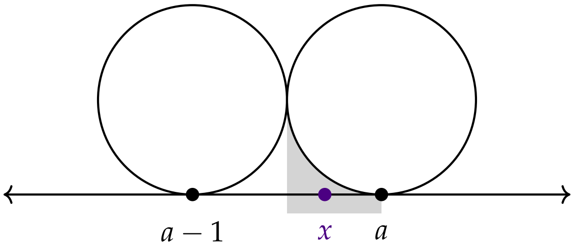
$$\frac{c}{d} \vee \frac{c'}{d'} = \frac{a}{b}$$

c/d and c'/d' occur in the sequence by the inductive hypothesis. Therefore, so does a/b as their mediant. □

Theorem 7.10 (Dirichlet's Approximation Theorem)**.** *Let x be an irrational real number. Then there exist infinitely many reduced fractions a/b such that*

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

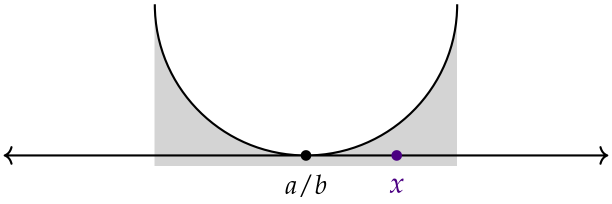
Proof. I. Start with $b = 1$, x is in the shadow of exactly Ford circle atop $\frac{a}{1}$



But then

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

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



Since x is an irrational real number, so either $x > a/b$ or $x < a/b$. Let's 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 7.4 we can find reduced fractions x/y and x'/y' with $y, y' < b$

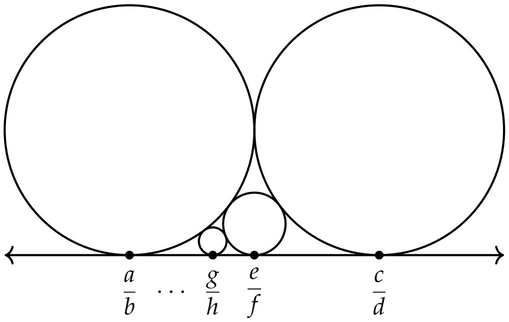
> such that a/b is their mediant. Let c/d be one of these fractions that lies to the right of a/b and by Lemma 7.9 we know that $c/d \heartsuit a/b$. □

Consider the chain

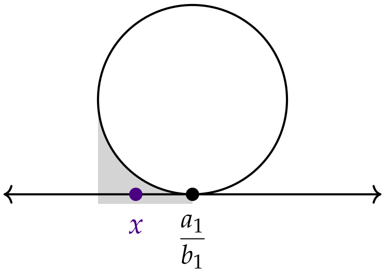
$$\frac{a}{b} \vee \frac{c}{d} = \frac{e}{f}$$

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

$$\vdots$$



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_1/b_1, where $b_1 < b$.



The radius of the circle $= \frac{1}{2}(\text{diameter}) = \frac{1}{2b_1^2}$. So,

$$\left| x - \frac{a_1}{b_1} \right| < \frac{1}{2b_1^2}$$

The case $x < a/b$ is similar (everything happens on the left). The theorem follows by starting with *I.* and repeatedly applying *II.* □

Remark 7.11 (Warning/Clarification)**.** The theorem doesn't imply that this approximation works for *every* integer b.

e.g. $\pi = 3.1415926\ldots$

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 $\frac{a}{b} = \frac{22}{7}$.

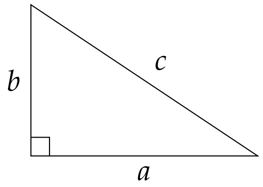
7.1. Problems

Problem 7.1. Write a formula which describes all fractions that kiss 7/11.

8. Lecture 8 (10/19)

Pythagorean Triples.

Definition 8.1. Let a, b, c be positive integers. Say (a, b, c) is a Pythagorean triple if $a^2 + b^2 = c^2$.



e.g. $(3, 4, 5)$, $(5, 12, 13)$

Goal. Find *all* Pythagorean triples.

Geometric Strategy. Start with equation

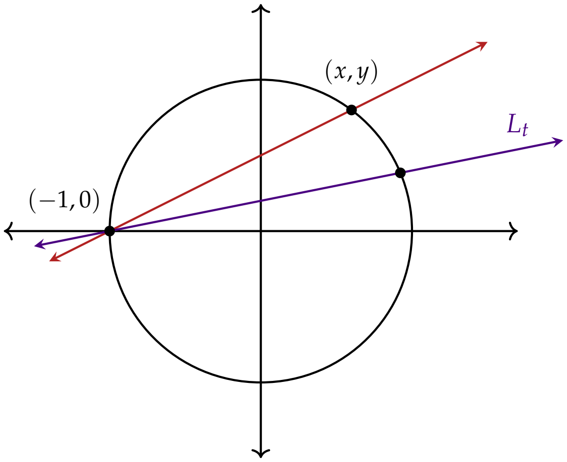
$$a^2 + b^2 = c^2$$

Dividing both sides by c^2, and letting $x := a/c$ and $y := b/c$. Then

$$x^2 + y^2 = 1$$

Since a, b, c are positive integers, x, y are rational and (x, y) lies on the unit circle! In other words, any Pythagorean triple gives rise to a rational point (points with rational coordinates) on the unit circle.

For such a point (x, y), consider the line passing through (x, y) and $(-1, 0)$. What can you say about the slope of this line?



Suppose we draw a line L_t through $(-1, 0)$ with rational slop t, what we can say about the point at which it intersects the unit circle C?

Proposition 8.2. *There's a bijection, where* $P_0 = (-1, 0)$

$$\left\{ P = (x,y) \in \mathbb{Q}^2 \;\middle|\; \begin{matrix} P \neq P_0 \\ x^2 + y^2 = 1 \end{matrix} \right\} \underset{g}{\overset{f}{\rightleftarrows}} \left\{ \begin{matrix} \textit{lines through } P_0 \\ \textit{with rational slope } t. \end{matrix} \right\}$$

Proof. Define

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

Note that L has rational slope: $\dfrac{y-0}{x-(-1)} = \dfrac{y}{x+1}$ is rational since x, y are rational numbers.

We now describe g: let L_t be the line through P_0 with rational slop t. Then L_t is defined by the equation

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

Let $(u,v) \in L_t \cap C$ then $v = t(u+1)$ and

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

As a quadratic equation in u, the equation above necessarily has two roots, say α and β. Crucial point is that $\alpha = -1$ is a root since $(-1, 0) \in L_t \cap C$. Since we know that

$$\alpha\beta = \frac{t^2-1}{1+t^2}, \quad \text{therefore } \beta = \frac{1-t^2}{1+t^2}$$

is the other root, i.e. $u = \dfrac{1-t^2}{1+t^2}$ is the x-coordinate of the other point in $L_t \cap C$. Then

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

Define $g(L_t) = \left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right) \in \mathbb{Q}^2$.

One readily checks f and g are inverses of each other. □

e.g. $t = 1/5$ corresponds to the Pythagorean triple $(12, 5, 13)$.

$$\begin{aligned} g(L_{1/5}) &= \left(\frac{1-(1/5)^2}{1+(1/5)^2}, \frac{2(1/5)}{1+(1/5)^2}\right) \\ &= \left(\frac{24}{26}, \frac{10}{26}\right) = \left(\frac{12}{13}, \frac{5}{13}\right) \end{aligned}$$

Modular Arithmetic

Sometimes, the remainder left after division can tell us a lot!

e.g. (1) Is $317 \times 694 = 219996$? *No, since the last digit should be* 8. $317 \times 694 = 219998$.

(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

$$x^2 + y^2 = 1234567 \tag{†}$$

have an integer solution?

Definition 8.3. 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 $m \mid (a - b)$, or equivalently $m \mid (b - a)$.

Congruence modulo m is an equivalence relation.

e.g. $317 \equiv 17 \bmod 10 \equiv 7 \bmod 10 \equiv -3 \bmod 10$

Proposition 8.4. *Let m be a modulus, and a, b, c, d are integers such that*

$$a \equiv b \bmod m \quad \text{and} \quad c \equiv d \bmod m.$$

Then $a + c \equiv b + d \bmod m$ and $ac \equiv bd \bmod m$.

Proof. (product) By assumption,

$$a - b = mr, \quad \text{for some } r \in \mathbb{Z}; \qquad\qquad c - d = ms, \quad \text{for some } s \in \mathbb{Z}$$

Then

$$\begin{aligned} ac &= (b + mr)(d + ms) \\ &= bd + m^2rs + m(dr + bs) \\ ac - bd &= m(mrs + dr + bs) \end{aligned}$$

Therefore $m \mid (ac - bd)$, and hence $ac \equiv bd \bmod m$. □

Definition 8.5. Let x be an integer and m a modulus, the *natural representative of x modulo m* is the remainder r left under the division algorithm

$$x = qm + r, \quad 0 \leqslant r < m.$$

Therefore $x \equiv r \bmod m$.

e.g. (1) Compute the natural representative modulo 10 of $1234567 \cdot 314159265$.

Hard way: Multiply this number and find out.

Easy way: Using Proposition 8.4,

$$\begin{aligned} 1234567 \cdot 314159265 &\equiv 7 \cdot 5 \bmod 10 \\ &\equiv 35 \bmod 10 \\ &\equiv 5 \bmod 10 \end{aligned}$$

(2) Compute the natural representative modulo 13 of 24^5.

First, $24 = 13 + 11 \equiv 11 \bmod 13 \equiv -2 \bmod 13$. Now, by Proposition 8.4,

$$\begin{aligned} 28^5 \equiv (-2)^5 \bmod 13 &\equiv -32 \bmod 13 \\ &\equiv 39 - 32 \bmod 13 \\ &\equiv 7 \bmod 13 \end{aligned}$$

(3) Compute the natural representative modulo 7 of 2^{10}.

(Attempt) $10 = 7 + 3 \bmod 7$, 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) $2 \equiv 2 \bmod 7,\ 2^2 \equiv 4 \bmod 7,\ 2^3 \equiv 8 \bmod 7 \equiv 1 \bmod 7$. So,

$$2^{10} = 2^3 \cdot 2^3 \cdot 2^3 \cdot 2 \equiv 1 \cdot 1 \cdot 1 \cdot 22 \bmod 7 \equiv 2 \bmod 7$$

Caution. In general, $b \equiv c \bmod m$ does *not* imply $a^b \equiv a^c \bmod m$.

Proposition 8.6. *Let N be a positive integer, and S be the sum of its digits. Then $N \equiv S \bmod 9$, and hence also $N \equiv S \bmod 3$.*

Proof. Let $N = d_0 + d_1 \cdot 10 + \cdots + d_k \cdot 10^k$, e.g. $247 = 7 + 4 \cdot 10 + 7 \cdot 100$. Then

$$\begin{aligned} N &= d_0 + d_1 \cdot 10 + \cdots + d_k \cdot 10^k \\ &\equiv d_0 + d_1 \cdot 1 + \cdots + d_k \cdot 1^k \bmod 9, \quad \text{by Proposition 8.4} \\ &\equiv d_0 + d_1 + \cdots + d_k \bmod 9 \\ &\equiv S \bmod 9 \end{aligned}$$

□

e.g. Note $247 \equiv 2 + 4 + 7 \bmod 9 \equiv 13 \bmod 9 \equiv 1 + 3 \bmod 9 \equiv 4 \bmod 9$.

Back to example (†). Does the equation $x^2 + y^2 = 1234567$ have an integer solution?

Answer. Strategy is to look at the equation modulo 4.

If z is an even integer, then $z = 2n$ for some integer n, and so

$$z^2 = (2n)^2 = 4n^2 \equiv 0 \bmod 4$$

If z is an odd integer, then $z = 2m + 1$ for some integer m, and so

$$z^2 = (2m+1)^2 = 4m^2 + 4m + 1 \equiv 1 \bmod 4$$

Therefore, if a solution (x, y) existed then $x, y \equiv 0, 1 \bmod 4$ and so $x^2 + y^2 \equiv 0, 1, 2 \bmod 4$.

But

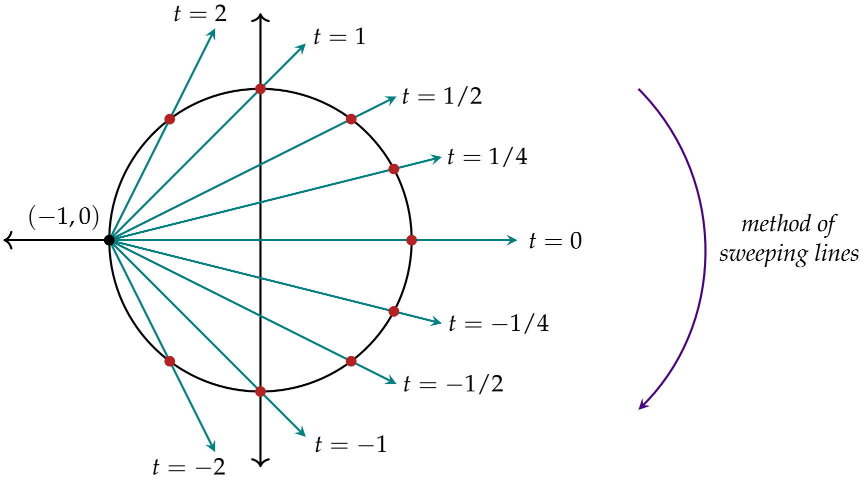
$$\begin{aligned} 1234567 &= 12345 \cdot 100 + 67 \\ &\equiv 67 \bmod 4 \\ &\equiv 64 + 3 \bmod 4 \\ &\equiv 3 \bmod 4 \end{aligned}$$

Thus, no solution exists. □

Solving Quadratic Equations, so far.

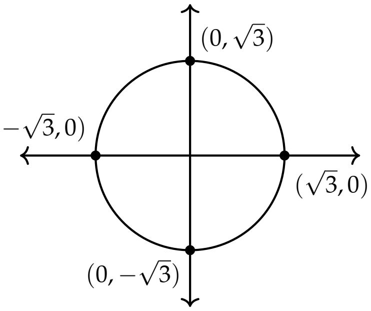
(1) $x^2 + y^2 = 1234567$ has no integer solutions.

(2) $x^2 + y^2 = z^2$ has infinitely many integer solutions, since we found all the rational solutions to the equation $X^2 + Y^2 = 1$.



(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?

Assume towards a contradiction that $(u,v) \in \mathbb{Q}^2$ is a solution of $x^2+y^2=3$, i.e.

$$u^2+v^2=3 \tag{$\star$}$$

Let c be the LCM of the denominators of x and y in their reduced form, and write

$$u=\frac{a}{c}, \quad v=\frac{b}{c} \tag{$\star\star$}$$

(*e.g.* if $u=3/10$ and $v=4/15$, then $c=\text{LCM}(10,15)=30$; rewrite as $u=9/30$ and $v=8/30$.)

Then $\text{GCD}(a,b,c)=1$ (see Problem 8.1) and $c \geqslant 1$.

Rewriting ($\star$) using ($\star\star$), we get

$$\frac{a^2}{b^2}+\frac{b^2}{c^2}=3 \iff a^2+b^2=3c^2 \tag{$\star\star\star$}$$

We want to now employ modular arithmetic, so for that a good modulus to choose will be 3. Since $a, b, c \in \mathbb{Z}$, we get

$$a^2+b^2=3c^2 \equiv 0 \bmod 3$$

Now, note that since $a \equiv 0,1,2 \bmod 3$, therefore $a^2 \equiv 0,1 \bmod 3$; similarly for $b^2 \bmod 3$. Hence, the only way we have $a^2+b^2 \equiv 0 \bmod 3$ is if $a^2 \equiv b^2 \equiv 0 \bmod 3$. Thus, $3 \mid a^2$ and $3 \mid b^2$, and so necessarily $3 \mid a$ and $3 \mid b$.

Let $a=3a_0$ and $b=3b_0$, substituting this in ($\star\star\star$) gives us

$$3c^2=(3a_0)^2+(3b_0)^2$$

$$c^2=3(a_0^2+b_0^2), \text{ necessarily}$$

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 $\mathrm{GCD}(a, b, c) = 1$. Hence we have arrived at a contradiction and thus $x^2 + y^2 = 3$ has no rational solutions.

8.1. Problems

Problem 8.1. Consider a pair of reduced fractions, N_u/D_u and N_v/D_v distinct as rational numbers. Let $c := \mathrm{LCM}(D_u, D_v)$ 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 $\mathrm{GCD}(a, b, c) = 1$.

Problem 8.2. Prove that there are infinitely many positive integer triples (x, y, z) such that

$$x^2 + 2y^2 = 3z^2.$$

Hint: find an appropriate rational point that will act as a "pivot", much like in the case of classifying Pythagorean triples that we saw in this lecture.

Problem 8.3. 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 in units place, thousands digit s, then $A = u - t + h - s + \cdots$. Then $N \equiv S \bmod 11$.

Problem 8.4.

(a) Let n be any integer. Prove that n^2 is congruent to 0, 1 or 4 modulo 8.

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

$$x^2 + y^2 + z^2 = 31415926535897932384626433832 7.$$

(c) Demonstrate that there are infinitely many positive integers that *cannot* be written as a sum of three squares.

Problem 8.5. 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 $a^{p^2} \equiv b^{p^2} \bmod p^3$.

(b) (challenge) Can you generalise?

Problem 8.6. Compute (the natural representative of) $3^{10^{10^{10}}} \bmod 7$.

Problem 8.7. Prove that a modulus m is even if and only if there exists an integer x such that $x \not\equiv 0 \bmod m$ and $x + x \equiv 0 \bmod m$.

Problem 8.8. Recall the Fibonacci numbers from Problem 6.2. Prove that for all $n \geqslant 1$,

$$F_n \equiv 4^{n-1}(2^n - 1) \bmod 11$$

9. Lecture 9 (10/21)

Notation. Let m be a modulus. By $\mathbb{Z}/m$ or $\mathbb{Z}/m\mathbb{Z}$ we mean the set of equivalence classes of integers with respect to the following (equivalence) relation

$$a \sim b \iff a \equiv b \bmod m$$

For any $a \in \mathbb{Z}$, its equivalence class will be denoted as $\overline{a}$ or $[a]$.

Essentially, $\overline{a}$ is the set that collects all integers that leave behind the same remainder as a when divided by m, i.e. have the same natural representative modulo m as a. Note that $\overline{a} = \overline{r}$, where r is the natural representative of a modulo m.

e.g. $m = 2$, $a = 1$,

$$\overline{1} = \{\dots, -3, -1, 1, 3, 5, \dots\} = \{1 + 2n \ : \ n \in \mathbb{Z}\}$$

$m = 5$, $a = 7$,

$$\overline{7} = \{\dots, -8, -3, 2, 7, 12, 17, \dots\} = \overline{2} = \{2 + 5n \ : \ n \in \mathbb{Z}\}$$

Proposition 8.4 can be recast as saying *addition and multiplication are well-defined operations on* $\mathbb{Z}/m\mathbb{Z}$ (i.e., $\mathbb{Z}/m\mathbb{Z}$ is a ring).

Division of integers modulo m.

(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 $\mathbb{Z}/m\mathbb{Z}$?

Definition 9.1. Let m be a modulus and a an integer. Say that $b \in \mathbb{Z}$ is a *multiplicative inverse of a modulo m* if

$$ab \equiv 1 \bmod m$$

e.g. $m = 11$ and $a = 4$. Then $b = 2$ is *not* a multiplicative inverse of a, since

$$ab = 8 \not\equiv 1 \bmod 11.$$

But $b = 3$ is, because $ab = 12 \equiv 1 \bmod 11$.

In fact, any other integer c such that $ac \equiv 1 \bmod 11$ will be of the form $3 + 11n$.

When a has a multiplicative inverse b modulo m, we can solve linear equations of the form

$$ax \equiv c \bmod m$$

easily.

Multiply by b, and you get $(ba)x \equiv bc \bmod m$. Since $ba \equiv 1 \bmod m$, we obtain $x \equiv (ba)x \equiv bc \bmod m$.

e.g. Let's solve $4x \equiv 7 \bmod 11$. We found $b = 3$ is a multiplicative inverse of 4 modulo 11, therefore

$$x \equiv (3 \cdot 4)x \equiv 3 \cdot (4x) \equiv 3 \cdot 7 \equiv 21 \equiv 10 \bmod 11$$

So, when does a given integer have a multiplicative inverse with respect to a given modulus?

Theorem 9.2. *Let m be a modulus and a an integer. Then*

(1) a has a multiplicative inverse modulo m if and only if $\mathrm{GCD}(a, m) = 1$.

(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 $ab \equiv 1 \bmod m$. So, $m \mid (ab - 1)$ and therefore $ab - 1 = mx$ for some $x \in \mathbb{Z}$. Hence $ab + m(-x) = 1$, and thus $\mathrm{GCD}(a, m) \mid 1$; so $\mathrm{GCD}(a, m) = 1$, necessarily.

($\Leftarrow$) Suppose $\mathrm{GCD}(a, m) = 1$, 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 9.3 (in-class)**.**

(1) Find the multiplicative inverse of 15 *modulo* 37.

(2) Using (1), solve the linear equation/congruence $15x \equiv 4$ *mod* 37.

Corollary 9.4. *$\overline{a}$ has a* unique *multiplicative inverse $\overline{b}$ in $\mathbb{Z}/m\mathbb{Z}$ if and only if* $\mathrm{GCD}(a, m) = 1$.

Corollary 9.5. *If* $\mathrm{GCD}(a,m) = 1$*, then for any* $x, y \in \mathbb{Z}$*,*

$$ax \equiv ay \text{ mod } m \implies x \equiv y \text{ mod } m$$

Corollary 9.6. *Let* p *be a prime number and* $a \in \mathbb{Z}$*. Then* a *has a multiplicative inverse modulo* p *if and only if* $p \nmid a$ *if and only if* $\overline{a} \neq \overline{0}$ *in* $\mathbb{Z}/p\mathbb{Z}$*.* $\mathbb{Z}/p\mathbb{Z}$ *is a field!*

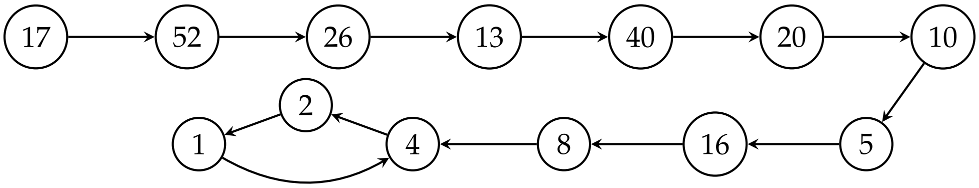
Modular Dynamics

Dynamics in the simplest mathematical form (discrete time): Let X be a set and $f : X \to X$ a function, what happens in this sequence x_0, $f(x_0)$, $f(f(x_0))$, $f(f(f(x_0))), \ldots, f^n(x_0), \ldots$?

e.g. Consider $X = \mathbb{N} = \mathbb{Z}_+ = \{1, 2, \ldots\}$, let $f : \mathbb{N} \to \mathbb{N}$ be defined as

$$f(n) = \begin{cases} n/2 & n \text{ is even} \\ 3n+1 & n \text{ is odd} \end{cases}$$

Say $x_0 = 17$, then the sequence reads: 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, ...



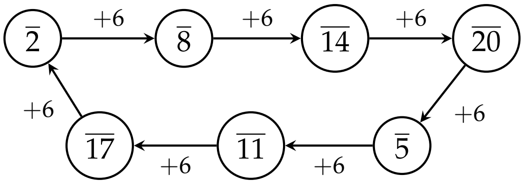
Conjecture 9.7 (Collatz, $3n+1$)**.** *For any* $x_0 \in \mathbb{N}$*, there exists a* $n > 0$ *such that* $f^n(x_0) = 1$*.*

Modular Dynamics. $X = \mathbb{Z}/m\mathbb{Z}$ or some subset of $\mathbb{Z}/m\mathbb{Z}$.

Additive Modular Dynamics.
For a modulus m and an integer a, we consider the dynamics of the function

$$\boxed{+a \text{ mod } m} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad \overline{x} \mapsto \overline{x+a}$$

e.g. Let $X = \mathbb{Z}/21\mathbb{Z}$, $a = 6$. We consider the dynamics of $\boxed{+6 \text{ mod } 21}$ with $x_0 = 2$,



this is a *cycle* of *length* 7.

Proposition 9.8. *Let m be a modulus and let a be an integer. Then the dynamics of* $\boxed{+a \bmod m}$ *consists of* $\operatorname{GCD}(a,m)$*-many cycles of length* $\ell = m/\operatorname{GCD}(a,m)$.

Proof. Suppose we start with $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$

$$\overline{b} \longrightarrow \overline{b+a} \longrightarrow \overline{b+2a} \longrightarrow \overline{b+3a} \longrightarrow \cdots \tag{$*$}$$

In step k, we get $\overline{b+ka}$.

Because $X = \mathbb{Z}/m\mathbb{Z}$ is a finite set, we return to $\overline{b}$ eventually (e.g. when $k = m$). Let ℓ be the smallest positive integer such that

$$\overline{b} = \overline{b + \ell a} \tag{$**$}$$

and ℓ is necessarily the length of the cycle ($*$).

Rewriting ($**$), we get $b \equiv b + \ell a \bmod m$; equivalently, $\ell a \equiv 0 \bmod m$. That is, $m \mid \ell a$ and ℓ is the smallest positive integer with this property. Therefore $\ell a = \operatorname{LCM}(a,m)$, and hence

$$\ell = \frac{\operatorname{LCM}(a,m)}{a} = \frac{m}{\operatorname{GCD}(a,m)}$$

So, the number of cycles $= m/\ell = \operatorname{GCD}(a,m)$. □

Corollary 9.9. *If* $\operatorname{GCD}(a,m) = 1$, *then* $\boxed{+a \bmod m}$ *on* $\mathbb{Z}/m\mathbb{Z}$ *has just* one *cycle of length* m.

9.1. Problems

Problem 9.1.

(1) Find the multiplicative inverse of 15 modulo 49.

(2) Using (1), solve the linear equation/congruence $15x \equiv 8 \bmod 49$.

Problem 9.2. Solve the congruences $5x \equiv 11 \bmod 37$ and $11y \equiv 5 \bmod 37$. If solutions exist, simplify $xy \bmod 37$.

Problem 9.3. Consider the following modular dynamical system, which is neither additive nor multiplicative.

(a) Let $X = \mathbb{Z}/13\mathbb{Z}$ and let $f : X \to X$ be given by

$$x \mapsto f(x) := x^2 + 3 \bmod 13.$$

Draw the complete diagram for the dynamics of f.

(b) Let $A_0 = 0$ and let $A_{n+1} = f(A_n) \bmod 13$ for all integers $n \geqslant 0$. What is $A_{2021} \bmod 13$?

10. Lecture 10 (10/26)

Multiplicative Modular Dynamics.

First complication: unlike additive modular dynamics, $\boxed{\times a \bmod m}$ is not reversible.

e.g.

$$\boxed{\times 12 \bmod 20} : \mathbb{Z}/20\mathbb{Z} \to \mathbb{Z}/20\mathbb{Z}, \quad \overline{n} \mapsto \overline{12n}$$

is *not* reversible (bijective). Since, $12x \equiv 1 \bmod 20$ doesn't have a solution as $\mathrm{GCD}(12, 20) = 4 \neq 1$.

Definition 10.1. Let m be a modulus. We define the following set

$$\Phi(m) = \{i \in \mathbb{Z} \ : \ 0 \leqslant i < m \text{ and } \mathrm{GCD}(i, m) = 1\} ;$$

it's the set of natural representatives of integers that are multiplicatively invertible modulo m.

We define the Euler's totient function $\varphi : \mathbb{Z} \to \mathbb{C}$ as $\varphi(m) := \#\Phi(m)$.

e.g. $\Phi(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$, so $\varphi(20) = 8$.

We restate the existence of multiplicative inverse modulo m

Proposition 10.2. *Let a be an integer between* 0 *and* $m - 1$ *(if not, consider that integer's natural representative modulo m; which, by definition, is an integer between* 0 *and* $m - 1$*).*

Then $a \in \Phi(m)$ *if and only if a has a multiplicative inverse modulo m if and only if* $\boxed{\times a \bmod m} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *is reversible (bijective).*

Proposition 10.3. *A modulus m is prime if and only if* $\varphi(m) = m - 1$*.*

Proof. ($\Rightarrow$) Suppose $m = p$ is prime, then $\Phi(p) = \{1, \ldots, p - 1\}$ since any positive integer less than p is necessarily coprime to it. Hence $\varphi(p) = \#\Phi(p) = p - 1$.

($\Leftarrow$) Suppose $\varphi(m) = m - 1$. Note that $m \neq 1$, since if $m = 1$, then $m - 1 = 0$ but $\varphi(m) = \varphi(1) = \#\Phi(1) = \#\{0\} = 1$. Hence $0 \notin \Phi(m)$, as the only number coprime to 0 is 1 (see Problem 1.2 (i)). Now, we clearly have $\Phi(m) \subseteq \{1, \ldots, m - 1\}$; furthermore, we've been given that $\#\Phi(m) = m - 1 = \#\{1, \ldots, m - 1\}$. Therefore, necessarily, $\Phi(m) = \{1, \ldots, m - 1\}$. Suppose m wasn't prime, then there exists an integer a such that $1 < a < m$ and $a \mid m$. Hence $a \in \{1, \ldots, m - 1\} = \Phi(m)$ but $\mathrm{GCD}(a, m) = a$, by Problem 1.2 (ii), contradicting the fact that $a \in \Phi(m)$. Thus, m is necessarily prime. □

Proposition 10.4. *If* $a, b \in \Phi(m)$*, then there exists a unique* $c \in \Phi(m)$ *such that* $ab \equiv c \bmod m$*. That is,* $\Phi(m)$ *is closed under multiplication modulo m).*

Proof. Take c to be the natural representative of ab modulo m, that is, the remainder left when we divide ab by m

$$ab = mq + c, \quad 0 \leqslant c < m$$

In particular, $ab \equiv c \bmod m$. We need to now show that $\text{GCD}(c, m) = 1$, we show this by producing a multiplicative inverse of c modulo m; see Theorem 9.2.

Since $\text{GCD}(a, m) = \text{GCD}(b, m) = 1$, by Theorem 9.2, there exist multiplicative inverses of a and b modulo m, say a' and b' respectively. That is,

$$aa' \equiv 1 \bmod m \quad \text{and} \quad bb' \equiv 1 \bmod m.$$

Note that,

$$\begin{aligned} c(a'b') &\equiv (ab)(a'b') \bmod m \\ &\equiv (aa')(bb') \bmod m \\ &\equiv 1 \bmod m \end{aligned}$$

Therefore $a'b'$ is a multiplicative inverse of c modulo m, and hence $c \in \Phi(m)$. Its uniqueness follows from the uniqueness of the remainder in the division algorithm. □

Dynamics of $\boxed{\times a \bmod m}$, when $a \in \Phi(m)$.

We focus on $X = \Phi(m)$. That is, we consider, for $a \in \Phi(m)$

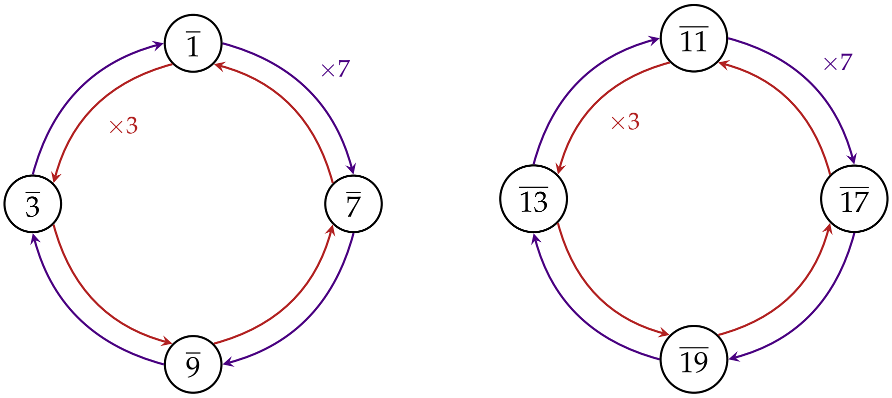
$$\boxed{\times a \bmod m} : \Phi(m) \to \Phi(m)$$

Let's start with an example, let's consider

$$\boxed{\times 7 \bmod 20} : \Phi(20) \to \Phi(20).$$

Note that $\Phi(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ and that 3 is the multiplicative inverse of 7 modulo 3.

We see that we get



Therefore, the dynamics of $\boxed{\times 7 \bmod 20}$ in the set $\Phi(20)$ has 2 cycles, each of length 4.

Lemma 10.5. *Let m be a modulus and $a \in \Phi(m)$. Then the dynamics of*

$$\boxed{\times a \bmod m} : \Phi(m) \to \Phi(m)$$

consists of cycles, all of the same length.

Proof. Initialising the dynamics at 1, we obtain a sequence of powers of a modulo m

$$1,\ a,\ a^2,\ a^3,\ \dots,\ a^n,\ \dots \tag{$\star$}$$

Since $\Phi(m)$ is a finite set, there must be repetition.

Say, $0 \leqslant e < f$ are integers such that $a^f \equiv a^e \bmod m$. Since $\mathrm{GCD}(a, m) = 1$, we necessarily have $\mathrm{GCD}(a^e, m) = 1$; rewriting the previous expression as $a^e \cdot a^{f-e} \equiv a^e \bmod m$, by Corollary 9.5, we obtain $a^{f-e} \equiv 1 \bmod m$.

Therefore, there's an integer $\ell = f - e > 0$ such that $a^\ell \equiv 1 \bmod m$. Let ℓ_0 be the smallest such positive integer.

> **Claim.** *If e, f are integers such that $0 \leqslant e < f < \ell_0$, then $a^e \not\equiv a^f$ mod m.*
>
> *Proof of Claim.* Suppose not, that is e, f are integers as given but $a^e \equiv a^f \bmod m$. Then similarly as before, by invoking Corollary 9.5, we obtain $a^{f-e} \equiv 1 \bmod m$. This contradicts the minimality of ℓ_0, since $f - e < \ell_0 - e < \ell_0$, therefore $a^e \not\equiv a^f \bmod m$. □

Thus, with this claim, we conclude that ($\star$) is a cycle of length ℓ_0.

Now, let $b \in \Phi(m)$ be arbitrary, and consider the sequence

$$b,\ ba,\ ba^2,\ ba^3,\ \dots,\ ba^n,\ \dots \tag{$\star_b$}$$

Since $a^{\ell_0} \equiv 1 \bmod m$, necessarily $ba^{\ell_0} \equiv b \bmod m$. Therefore, ($\star_b$) is a cycle of length less than or equal to ℓ_0. Suppose the length of ($\star_b$) was $k < \ell_0$, that is, $ba^k \equiv b \bmod m$. Then, since $\mathrm{GCD}(b, m) = 1$, by Corollary 9.5 we obtain $a^k \equiv \bmod m$. This contradicts the minimality of ℓ_0, and hence ($\star_b$) must also have length ℓ_0. □

10.1. Problems

Problem 10.1.

(a) Compute the length of the cycles in the dynamics of $\boxed{\times a \bmod 8}$ for every $a \in \Phi(8)$. Compare the length with $\varphi(8)$.

(b) Compute the length of the cycles in the dynamics of $\boxed{\times 3 \bmod 14}$. Compare the length with $\varphi(14)$.

11. Lecture 11 (10/28)

Theorem 11.1 (Euler-Fermat)**.** *Let m be a modulus and $a \in \Phi(m)$. Then*

$$a^{\varphi(m)} \equiv 1 \textit{ mod } m$$

Proof. Consider the dynamics of $\boxed{\times a \text{ mod } m}$ in $\Phi(m)$. We have seen in Lemma 10.5 that all cycles have the same length, say ℓ_0. In particular, initialising at 1 we obtain

$$a^{\ell_0} \equiv 1 \text{ mod } m. \tag{1}$$

One the other hand, let c be the number of cycles in the dynamical system. Then, since $\#\Phi(m) = \varphi(m)$, necessarily

$$\varphi(m) = c\ell_0. \tag{2}$$

Therefore,

$$a^{\varphi(m)} \underset{(2)}{=} (a^{\ell_0})^c \underset{(1)}{\equiv} 1^c \equiv 1 \text{ mod } m$$

□

Corollary 11.2 (Fermat's little theorem)**.** *Given a prime p, let $a \in \Phi(p)$, then*

$$a^{p-1} \equiv 1 \textit{ mod } p;$$

since $\varphi(p) = p - 1$. If we rewrite the above expression as $a^p \equiv a$ mod p, this holds true even for $a = 0$.

Example 11.3. *Simplify* 2^{2021} *mod* 9

Answer. Note $\Phi(9) = \{1, 2, 4, 5, 7, 8\}$; so $\varphi(9) = 6$ and therefore $2^6 \equiv 1$ mod 9 since $\text{GCD}(2, 9) = 1$. Now, $2021 = 336 \cdot 6 + 5$; so

$$\begin{aligned} 2^{2021} &= (2^6)^{336} \cdot 2^5 \\ &\equiv 2^5 \text{ mod } 9 \\ &\equiv 5 \text{ mod } 9 \end{aligned}$$

On the other hand, $3^6 = 9^3 \equiv 0 \text{ mod } 9 \not\equiv 1 \text{ mod } 9$, since $\text{GCD}(3, 9) \neq 1$. □

Corollary 11.4. *Let m be a modulus and $a \in \Phi(m)$. Then, for any integer b, c such that $b \equiv c$ mod $\varphi(m)$, we have*

$$a^b \equiv a^c \textit{ mod } m$$

Application: Primality Testing. Given a number N, 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 11.5. *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 $a \mid N$. □

e.g. If $N \sim 2^{2000}$, we only need to check for divisors upto $\sqrt{N} \sim 2^{1000}$.

One consequence of Corollary 11.2 is that if, for some $1 < a < N$, we have $a^{N-1} \equiv 1 \bmod N$, then N cannot be prime.

Caution: the converse is not true, there exist composite numbers M such that $x^{M-1} \equiv 1 \bmod M$ for any integer x coprime to M; for instance, $M = 561$. Such numbers are called Carmichael numbers *or (absolute) Fermat pseudoprimes.*

Theorem 11.6. *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 $\varphi(n) = \#\Phi(n)$, where

$$\Phi(n) = \{i \in \mathbb{Z} \,:\, 0 \leqslant i < n,\ \mathrm{GCD}(i, n) = 1\}.$$

Consider the sets

$$\begin{aligned} A &= \{0, 1, \ldots, n-1\} \\ B_1 &= \{a \in A \,:\, p_1 \mid a\} \\ B_2 &= \{a \in A \,:\, p_2 \mid a\} \\ &\vdots \\ B_t &= \{a \in A \,:\, p_t \mid a\} \end{aligned}$$

Note that

$$\begin{aligned} \Phi(n) &= \{a \in A \,:\, p_i \nmid a,\ \text{for all } i = 1, \ldots, t\} \\ &= \{a \in A \,:\, a \notin B_i,\ \text{for all } i = 1, \ldots, t\} = A \setminus \cup_{i=1}^{t} B_i, \end{aligned}$$

so we need to compute

$$\#\big(A \setminus \cup_{i=1}^{t} B_i\big) = \#A - \#\big(\cup_{i=1}^{t} B_i\big) = n - \#\big(\cup_{i=1}^{t} B_i\big),$$

in particular $\#\left(\cup_{i=1}^{t} B_i\right)$; which, by the inclusion – exclusion principle, is

$$\#\left(\bigcup_{i=1}^{t} B_i\right) = \left(\sum_{k=1}^{t} (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant t} \#\left(B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_k}\right)\right)$$

For that, take any choice of indices $1 \leqslant i_1 < \cdots < i_k \leqslant t$ and we claim

$$\#(B_{i_1} \cap \cdots \cap B_{i_k}) = \frac{n}{p_{i_1} \cdots p_{i_k}}$$

Since the primes $p_1, \ldots, p_t$ are distinct, we have

$$\begin{aligned} B_{i_1} \cap \cdots \cap B_{i_k} &= \left\{ a \in A \ : \ p_{i_1} \mid a, \ldots, p_{i_k} \mid a \right\} \\ &= \left\{ a \in A \ : \ p_{i_1} \cdots p_{i_k} \mid a \right\} \\ &= \left\{ p_{i_1} \cdots p_{i_k} b \ : \ 0 \leqslant b < n/(p_{i_1} \cdots p_{i_k}) \right\} \end{aligned}$$

We explicitly prove the last equality; clearly the latter set is a subset of the former. Consider an element of the former, i.e., an $c \in A$ such that $p_{i_1} \cdots p_{i_k} \mid c$, then $c = p_{i_1} \cdots p_{i_k} d$, for some $d \in \mathbb{Z}$. Since $c \in A$, we have $0 \leqslant c = p_{i_1} \cdots p_{i_k} d < n$, which shows that $0 \leqslant d < n/(p_{i_1} \cdots p_{i_k})$. Therefore $c = p_{i_1} \cdots p_{i_k} d$ is an element of the latter set, and hence our equality of sets in the last step is justified.

Hence $\#(B_{i_1} \cap \cdots \cap B_{i_k}) = \dfrac{n}{p_{i_1} \cdots p_{i_k}}$, as claimed.

We return to our calculations,

$$\begin{aligned} \varphi(n) &= \#\Phi(n) \\ &= n - \left(\sum_{k=1}^{t} (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant t} \#(B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_k}) \right) \\ &= n - \left(\sum_{k=1}^{t} (-1)^{k+1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant t} \frac{n}{p_{i_1} \cdots p_{i_k}} \right) \\ &= n \left(1 - \left(\frac{1}{p_1} + \cdots + \frac{1}{p_2} \right) + \left(\sum_{1 \leqslant i_1 < i_2 \leqslant t} \frac{1}{p_{i_1} p_{i_2}} \right) + \cdots + (-1)^t \frac{1}{p_1 \cdots p_t} \right) \\ &= n \left(1 - \frac{1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \cdots \left(1 - \frac{1}{p_t} \right) \end{aligned}$$

Hence $\varphi(n) = n \left(1 - \dfrac{1}{p_1} \right) \left(1 - \dfrac{1}{p_2} \right) \cdots \left(1 - \dfrac{1}{p_t} \right)$. □

Corollary 11.7. *Let p be a prime, then $\varphi(p^e) = p^{e-1}(p-1)$ for any integer $e \geqslant 1$.*

Corollary 11.8. *φ is multiplicative. That is, for positive integers a, b such that* $\operatorname{GCD}(a,b) = 1$, *we have*

$$\varphi(ab) = \varphi(a)\varphi(b)$$

Example 11.9 (in-class). *Compute $\varphi(72)$, and then compute (the natural representative of) 5^{2403} mod 72.*

11.1. Problems

Problem 11.1. Compute (the natural representative of) $3^{10^{10^{10}}}$ mod 7.

Problem 11.2. 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 a divisor either of $2^p - 1$ or of $2^p + 1$, but not of both.

Problem 11.3. Suppose that p is a prime and $p \equiv 2 \bmod 3$. 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 11.4. Consider the recursive sequence given by

$$a_0 = 3, \quad a_n = 3^{a_{n-1}}, \text{ for } n \geqslant 1$$

That is, $a_0 = 3$, $a_1 = 3^3$, $a_2 = 3^{3^3}$, ... What is the last digit of a_{1000}?

12. Lecture 12 (11/2)

Recall from Problem 4.8 that given two multiplicative functions $f, g : \mathbb{Z}_+ \to \mathbb{C}$, the function, that we called *convolution*, $(f * g) : \mathbb{Z}_+ \to \mathbb{C}$, defined as

$$(f * g)(n) := \sum_{d \in \mathscr{D}(n)} f(d) g\left(\frac{n}{d}\right),$$

is also multiplicative.

Take $f = \mu$, the Möbius function (see Problem 4.7) and $g = \mathrm{id}$, i.e., $g(n) = n$ for all positive integers n. Then,

$$\begin{aligned}
(\mu * \mathrm{id})(p^e) &= \sum_{d \in \mathscr{D}(p^e)} \mu(d)\, \mathrm{id}\left(\frac{n}{d}\right) \\
&= \sum_{k=0}^{e} \mu(p^k) \left(\frac{p^e}{p^k}\right) \\
&= \mu(1) p^e + \mu(p) p^{e-1} + \sum_{k=2}^{e} \mu(p^k) \left(\frac{p^e}{p^k}\right) \\
&= p^e - p^{e-1}, \quad \text{since } \mu(p^k) = 0, \text{ for } k \geqslant 2 \\
&= p^{e-1}(p-1) \\
&= \varphi(p^e)
\end{aligned}$$

Hence, by multiplicativity of $\mu * \mathrm{id}$ and φ, we conclude that $\mu * \mathrm{id} = \varphi$

Lemma 12.1. *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 12.1. From Problem 4.7 we know that

$$\sum_{d \in \mathscr{D}(n)} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases} \tag{$\bigstar$}$$

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 ($\bigstar$) can be rewritten as follows

$$(\mu * \mathbb{1})(n) = \sum_{d \in \mathscr{D}(n)} \mu(d)\, \mathbb{1}\left(\frac{n}{d}\right) = \sum_{d \in \mathscr{D}(n)} \mu(d) \cdot 1 = \sum_{d \in \mathscr{D}(n)} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

Note that this tells us that $\mu * \mathrm{id} = \varepsilon$, where ε is as defined in Problem 12.1. Similarly,

$$\sum_{d \in \mathscr{D}(n)} \varphi(d) = (\varphi * \mathbb{1})(n)$$

Now, again by Problem 12.1, 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, $\displaystyle\sum_{d \in \mathscr{D}(n)} \varphi(d) = (\varphi * \mathbb{1})(n) = \mathrm{id}(n) = n.$ □

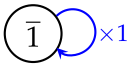
Primitive Roots and Polynomials. Let p be prime and $a \in \Phi(p)$ (equivalently, $p \nmid a$). We define $\ell(a)$ as the length of the cycles in the dynamics of $\boxed{\times a \bmod p}$ within $\Phi(p)$.

We have seen, while proving Theorem 11.1 (Euler-Fermat), that $\ell(a) \mid \varphi(p) = p - 1$.

Definition 12.2. Say a is a primitive root modulo p if $\ell(a) = p - 1$. Equivalently, if there's only one cycle in the dynamics of $\boxed{\times a \bmod p}$ within $\Phi(p)$.

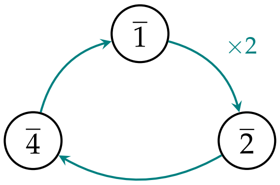
e.g. $p = 7$

$a = 1$



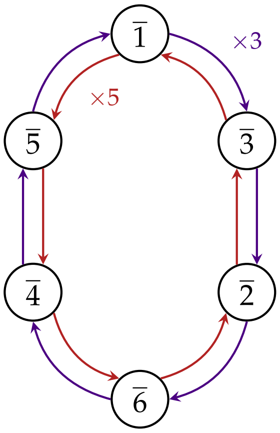
$\ell(1) = 1 \neq 7 - 1$, so 1 is *not* primitive.

$a = 2$



$\ell(2) = 3 \neq 7 - 1$, so 2 is *not* primitive.

$a = 3$



$\ell(3) = 6 = 7 - 1$, so 3 *is primitive.*

So is 5, as the multiplicative inverse of 3 modulo 7 in $\Phi(7)$.

Our goal is to prove

Theorem (Gauss)**.** *Let p be a prime number, then there exist primitive roots in $\Phi(p)$, and there are precisely $\varphi(p-1)$-many of them.*

e.g. For $p = 7$, $\varphi(7-1) = \varphi(6) = \varphi(2)\varphi(3) = 1 \cdot 2 = 2$. The theorem tells us that there are 2 primitive roots modulo 7, they're necessarily 3 and 5, as seen in the example above.

Notation. For p a prime, we let $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$.

Furthermore, $\mathbb{F}_p^\times := (\mathbb{Z}/p\mathbb{Z}) \setminus \{\overline{0}\} = \{\overline{1}, \ldots, \overline{p-1}\}$; note that that the set of representatives of this set is exactly $\Phi(p)$.

Definition 12.3. 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 $\mathbb{F}_p$.

Convention: $\deg 0 := -1$, where 0 is the zero polynomial.

We can add, subtract and multiply polynomials modulo p; that is, $\mathbb{F}_p[T]$ is a ring.

e.g. $p = 5$

$$f(T) = \overline{4}T + \overline{2} \qquad\qquad g(T) = \overline{3}T^2 + \overline{2}T$$

$$\deg f = 1 \qquad\qquad \deg g = 2$$

$$\begin{aligned} f(T)g(T) &= (\overline{4}T + \overline{2})(\overline{3}T^2 + \overline{2}T) \\ &= \overline{12}T^3 + \overline{6}T^2 + \overline{8}T^2 + \overline{4}T \\ &= \overline{12}T^3 + \overline{14}T^2 + \overline{4}T \\ &= \overline{2}T^3 + \overline{4}T^2 + \overline{4}T = \overline{2}T^3 - T^2 - T, \quad \text{reducing mod 5} \end{aligned}$$

Theorem 12.4. *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

$$f(T) = a_d T^d + (\text{terms}), \quad a_d \neq \overline{0}$$

$$g(T) = b_e T^e + (\text{terms}), \quad b_e \neq \overline{0}$$

Then $f(T)g(T) = a_d b_e T^{d+e} + (\text{terms})$. Since $a_d, b_e \neq \overline{0}$ in $\mathbb{F}_p$, where p is prime, necessarily $a_d b_e \neq \overline{0}$. Therefore $\deg(fg) = d + e = \deg f + \deg g$. □

Remark 12.5. If m was composite, then we can similarly consider polynomials modulo m and we can add, subtract and multiply such polynomials. But the previous theorem does not hold.

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,

$$f(T)g(T) = \overline{4}T^3 + \overline{6}T^4 = \overline{4}T^3 + \overline{0}T^4 = \overline{4}T^3.$$

Then $\deg(fg) = 3 \neq 4 = \deg f + \deg g$.

12.1. Problems

Problem 12.1. Let $f(n)$ and $g(n)$ be two complex-valued functions of positive integers $n > 0$. 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: ε acts as the neutral element for the convolution.)

(c) Let $h : \mathbb{Z}_+ \to \mathbb{C}$ be a third 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

$$i_f(1) := \frac{1}{f(1)}. \tag{12.1.d.1}$$

Given an integer $n > 1$, assume we have defined $i_f(d)$ for all the proper positive divisors d of n, this is the set $\mathscr{D}_{\mathrm{pr}}(n) := \mathscr{D}(n) \setminus \{n\}$. Then proceed to define

$$i_f(n) := -\frac{1}{f(1)} \sum_{d \in \mathscr{D}_{\mathrm{pr}}(n)} i_f(d) f\left(\frac{n}{d}\right). \tag{12.1.d.2}$$

Compute $i_f(n)$ for $n = 2, 3, 4, 5, 6$ in the particular case where f is the identity function: $f(n) = n$.

(e) Return to the general case where $f(n)$ is any function such that $f(1) \neq 0$, and i_f is defined by the formulae (12.1.d.1) and (12.1.d.2).

Prove that $i_f * f = \varepsilon$.

Prove that if $j(n)$ is any other complex valued function such that $j * f = \varepsilon$, then we necessarily have $j = i_f$.

Hint: look back to our proof of “uniqueness" of multiplicative inverses modulo m.

Problem 12.2 (Möbius Inversion)**.** Let f and g be two arithmetic functions, that is $f, g : \mathbb{Z}_+ \to \mathbb{C}$. Prove that

$$g(n) = \sum_{d \in \mathscr{D}(n)} f(d) \quad \text{if and only if} \quad f(n) = \sum_{d \in \mathscr{D}(n)} \mu(d) g\left(\frac{n}{d}\right)$$

In the language of convolution, the question is asking you to prove that

$$g = f * \mathbb{1} \quad \text{if and only if} \quad f = g * \mu$$

This is sometimes called the Möbius Inversion formula. You can now probably see that Lemma 12.1 was just an application of this.

Consider the arithmetic function defined as $p_k(n) = n^k$; in particular, $p_0 = \mathbb{1}$ and $p_1 = \text{id}$. Using Möbius Inversion, prove that

$$p_k = \sigma_k * \mu.$$

Problem 12.3.

(a) Compute $\ell(a)$ in the 3×4 cases: $a = 2, 3, 6$ and $p = 7, 11, 13, 17$.

(b) For the primes $p = 7, 11, 13, 17$, list all the primitive roots modulo p.

13. Lecture 13 (11/4)

Definition 13.1. 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.

e.g. Consider $p = 5$, $g(T) = \overline{3}T^2 + \overline{2}T$

- $a = \overline{0}$ is a root of $g(T)$, since $g(\overline{0}) = \overline{0}$.
- $a = \overline{1}$ is a root of $g(T)$, since $g(\overline{1}) = \overline{3} \cdot \overline{1}^2 + \overline{2} \cdot \overline{1} = \overline{5} = \overline{0}$.
- $a = \overline{2}$ 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 13.2. *Consider a linear polynomial $f(T) = aT + b \in \mathbb{F}_p[T]$, in particular $a \neq \overline{0}$ in $\mathbb{F}_p$. Then $f(T)$ has a unique root in $\mathbb{F}_p$.*

Proof. Since $a \neq \overline{0}$, there exists a unique $c \in \mathbb{F}_p$ such that $ac = 1$, by Corollary 9.6. Now, let $x \in \mathbb{Z}$, 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 $\overline{x} = -cb$. □

The set of polynomials modulo p, $\mathbb{F}_p[T]$, behaves a lot like $\mathbb{Z}$.

Theorem 13.3 (Division algorithm in polynomials modulo p)**.** *Let p be a prime, and $f(T), g(T) \in \mathbb{F}_p[T]$. Assume that $g(T)$ is not the zero polynomial ($\deg g \geqslant 0$). Then there exist polynomials modulo p, $q(T)$ and $r(T)$, such that*

$$f(T) = g(T)q(T) + r(T), \quad \deg r < \deg g$$

e.g. Consider $p = 5$ and polynomials $f(T) = T^3 + \overline{4}T + \overline{2}$, $g(T) = T^2 + T + \overline{2}$

$$\begin{array}{r l l}
 & \quad T - \overline{1} & \\
T^2 + T + \overline{2}\,\big) & \overline{T^3 + \overline{0}T^2 + \overline{4}T + \overline{2}} & \\
 & \underline{T^3 + \ T^2 + \overline{2}T} & \text{(subtract)} \\
 & \quad - \ T^2 + \overline{2}T + \overline{2} & \\
 & \underline{\quad - \ T^2 - \ T - \overline{2}} & \text{(subtract)} \\
 & \qquad\qquad \overline{3}T + \overline{4} &
\end{array}$$

Therefore

$$f(T) = \underbrace{(T - \overline{1})}_{q(T)} g(T) + \underbrace{(\overline{3}T + \overline{4})}_{r(T)}$$

Definition 13.4. Let p be a prime number, and polynomial below means polynomial modulo p

- A *unit polynomial* is a non-zero constant polynomial, that is a polynomial of degree 0.

- A polynomial $f(T)$ is an *irreducible polynomial* if

  (IR1) $\deg f \geqslant 1$ (non-constant, equivalently non-unit); and

  (IR2) 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.

Here, we have an 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 13.5. *For any $a \in \mathbb{F}_p$, the linear polynomial $f(T) = T - a \in \mathbb{F}_p[T]$ is irreducible.*

Answer. Clearly (IR1) of Definition 13.4 is met. Let's prove (IR2); suppose

$$T - a = g(T)h(T),$$

then $1 = \deg(T - a) = \deg g + \deg h$. Therefore, $\deg g = 0$ and $\deg h = 1$, or vice versa (since $f \neq 0$). Hence $g(T)$ is a unit, or $h(T)$ is. Thus, $f(T)$ is irreducible. □

In fact, there are infinitely many polynomials modulo p. One proves this similarly as one proves the infinitude of primes once one has Theorem 13.7.

Definition 13.6. Let p be a prime and $f(T) \in \mathbb{F}_p[T]$. Let $d = \deg f$, and write

$$f(T) = a_d T^d + \cdots + a_1 T + a_0$$

Then a_d is called 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 13.7 (Unique factorisation in polynomials modulo p)**.** *Let $f(T)$ be a non-zero polynomials modulo p, where p is prime. Then $f(T)$ can be uniquely written as*

$$f(T) = c \cdot p_1(T)^{e_1} p_2(T)^{e_2} \cdots p_r(T)^{e_r}$$

where

- *c is the leading coefficient of $f(T)$;*
- *$p_1(T), p_2(T), \ldots, p_r(T)$ are monic irreducible polynomials modulo p; and*

- *$e_1, \ldots, e_r > 0$ are integers.*

Proof. The proof is similar to the proof of uniqueness of prime factorisation in $\mathbb{Z}$, Theorem 2.11. One applies (strong) induction on $\deg f$. □

Lemma 13.8. *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 algorithm to $f(T)$ and $T - \overline{x}$,

$$f(T) = (T - \overline{x})q(T) + r(T),$$

where $q(T), r(T) \in \mathbb{F}_p[T]$ and $\deg r < \deg(T - \overline{x}) = 1$. Therefore $\deg r = 0$ or -1, i.e., $r(T)$ is a unit (a constant polynomial) or the zero polynomial. Say, $r = r(T) \in \mathbb{F}_p$; so we have

$$f(T) = (T - \overline{x})q(T) + r$$

Evaluating the above equation at $\overline{x}$ gives us

$$f(\overline{x}) = (\overline{x} - \overline{x})q(\overline{x}) + r = r.$$

Hence, $f(T)$ has x as a root if and only if $f(\overline{x}) = 0$ if and only if $r = 0$. Thus, $f(T)$ has $\overline{x}$ as a root if and only if $f(T) = (T - \overline{x})q(T)$ if and only if $T - \overline{x}$ divides $f(T)$. □

Theorem 13.9. *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 $\deg f$. If $\deg f = 1$, then $f(T) = aT + b$ with $a \neq \overline{0}$. Then, by Proposition 13.2, f has a unique root in $\mathbb{F}_p$. Hence, the base case holds.

Assume the induction hypothesis. Suppose $f(T)$ has no roots in $\mathbb{F}_p$, then nothing to prove and the result holds (since $0 \leqslant \deg f$).

Therefore, assume f has a root, say $a \in \mathbb{F}_p$. Then, by Lemma 13.8, we have $f(T) = (T - a)g(T)$, for some polynomial $g(T) \in \mathbb{F}_p[T]$. So, $\deg g = \deg f - 1$, by Theorem 12.4.

Therefore, by the induction hypothesis, $g(T)$ has at most $(\deg g)$-many distinct roots. Note that

$$\{\text{roots of } f(T)\} = \{a\} \cup \{\text{roots of } g(T)\}$$

Hence,

$$\begin{aligned}\#\{\text{roots of } f(T)\} &\leqslant \#\{a\} + \#\{\text{roots of } g(T)\}\\ &\leqslant 1 + \deg g\\ &= 1 + (\deg f - 1)\\ &= \deg f\end{aligned}$$

Thus, the result holds, by the principle of mathematical induction. □

Remark 13.10. As in a similar case before, the assumption that p is prime is important. If m was composite, then we can similarly 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 polynomial $f(T) = T^2 - \overline{1}$ modulo 8. Note that

$$f(\overline{1}) = \overline{1}^2 - \overline{1} = \overline{0}$$

$$f(\overline{3}) = \overline{3}^2 - \overline{1} = \overline{8} = \overline{0}$$

$$f(\overline{5}) = \overline{5}^2 - \overline{1} = \overline{24} = \overline{0}$$

$$f(\overline{7}) = \overline{7}^2 - \overline{1} = \overline{48} = \overline{0}$$

Clearly $\overline{1}$, $\overline{3}$, $\overline{5}$ 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.

13.1. Problems

Problem 13.1.

(a) Let $f(T)$ be an irreducible polynomial modulo p, and consider any $a \in \mathbb{F}_p$ such that $a \neq \overline{0}$. Prove that $g(T) := af(T)$ 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 theorem from class.

Give an example illustrating why this reasoning does not help us determine if a given polynomial (modulo p) of degree $\geqslant 4$ is irreducible.

Problem 13.2. Let $p = 5$ and consider two polynomials mod p:

$$f(T) = T^3 + \overline{3}T^2 + \overline{2}T + 1$$

$$g(T) = \overline{2}T^4 + \overline{4}T^3 + T^2 + \overline{3}T + \overline{4}.$$

(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 13.1.

(d) Find the unique decompositions of $f(T)$ and $g(T)$ into irreducible polynomials mod p.

14. Lecture 14 (11/9)

Example 14.1. *Consider the polynomial $f(T) = T^3 + \overline{2} \in \mathbb{F}_5[T]$, let's find the unique factorisation into irreducibles of f.*

Answer. First, we check if $f(T)$ has a root modulo 5; note

a	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$f(a)$	$\overline{2}$	$\overline{1}+\overline{2}=\overline{3}$	$\overline{8}+\overline{2}=\overline{0}$	$\overline{27}+\overline{2}=\overline{4}$	$\overline{64}+\overline{2}=\overline{1}$

Therefore $\overline{2}$ is a root of $f(T)$, hence by Corollary 13.8 we have that $T-\overline{2}$ divides $f(T)$. Thus,

$$f(T) = (T-\overline{2})g(T),$$

for some polynomial $g(T) \in \mathbb{F}_5[T]$ and $\deg g = 2$. We employ long division to compute $g(T)$

$$\begin{array}{rll}
 & T^2 + \overline{2}T + \overline{4} & \\
T-\overline{2}\,\big) & T^3 + \overline{0}T^2 + \overline{0}T + \overline{2} & \\
 & \underline{T^3 - \overline{2}T^2} & \text{(subtract)} \\
 & \quad \overline{2}T^2 + \overline{0}T + \overline{2} & \\
 & \quad \underline{\overline{2}T^2 - \overline{4}T} & \text{(subtract)} \\
 & \qquad \overline{4}T + \overline{2} & \\
 & \qquad \underline{\overline{4}T - \overline{8}} & \text{(subtract)} \\
 & \qquad\qquad \overline{10} = \overline{0} &
\end{array}$$

Therefore $g(T) = T^2 + \overline{2}T + \overline{4}$, hence

$$f(T) = (T-\overline{2})(T^2+\overline{2}T+\overline{4}) = (T+\overline{3})(T^2+\overline{2}T+\overline{4})$$

Note,

a	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$g(a)$	$\overline{4}$	$\overline{7}=\overline{2}$	$\overline{12}=\overline{2}$	$\overline{19}=\overline{4}$	$\overline{28}=\overline{3}$

Thus, by Problem 13.1, $g(T)$ is irreducible since it has no roots modulo 5. Therefore the factorisation that we obtained for $f(T)$ is its factorisation into irreducibles. □

Definition 14.2 (Recall)**.** Let p be a prime number and $a \in \Phi(p)$, then

- $\ell(a) =$ the common length of the cycles in the dynamics of $\boxed{\times a \bmod p}$ in $\Phi(p)$

  $=$ the smallest positive integer ℓ such that $a^\ell \equiv 1 \bmod p$

- $c(a) =$ the number of cycles in the dynamics of $\boxed{\times a \bmod p}$ in $\Phi(p)$

In the course of proving Theorem 11.1, we noted that $c(a) \cdot \ell(a) = \#\Phi(p) = \varphi(p) = p-1$.

Lemma 14.3. *Let p be a prime and $\lambda > 0$ be an integer; define*

$$\Phi_\lambda(p) := \{a \in \Phi(p) \ : \ \ell(a) = \lambda\}$$

Then, the set $\Phi_\lambda(p)$ has either 0 (that is, the set is empty) or $\varphi(\lambda)$-many elements.

Proof. Suppose $\Phi_\lambda(p)$ is non-empty, we must prove that $\#\Phi_\lambda(p) = \varphi(\lambda)$. So, let $a \in \Phi_\lambda(p)$, in particular $\ell(a) = \lambda$.

Then, for $e = 0, 1, \ldots, \lambda - 1$, we have

$$(a^e)^\lambda = (a^\lambda)^e \equiv 1^e \equiv 1 \bmod p$$

Therefore, the polynomial $f(T) = T^\lambda - \overline{1} \in \mathbb{F}_p[T]$ has $a^0, a^1, \ldots, a^{\lambda-1}$ as roots. Moreover, since $\ell(a) = \lambda$, these are necessarily distinct modulo p.

Since $\deg f = \lambda$ and we found λ-many distinct roots of f, the set $R_a = \{a^e \ : \ 0 \leqslant e < \lambda\}$ necessarily consists of all roots of f, and thus

$$T^\lambda - \overline{1} = (T - \overline{a}^0)(T - \overline{a}^1) \cdots (T - \overline{a}^{\lambda-1})$$

Now, if $b \in \Phi_\lambda(p)$ was arbitrary, then by assumption $\ell(b) = \lambda$ and so $b^\lambda \equiv 1 \bmod p$. Hence, b is a root of $T^\lambda - \overline{1}$, and therefore, necessarily, $\overline{b} = \overline{a}^e$, for some $e = 0, 1, \ldots, \lambda - 1$.

Thus, to count $\Phi_\lambda(p)$, it suffices to focus on a^e. So, the question we want to ask is: what is $\ell(a^e)$? As this answer will tell us for what e is $a^e \in \Phi_\lambda(p)$.

If $k > 0$ is an integer such that $(a^e)^k \equiv 1 \bmod p$, then

$$a^{ek} \equiv 1 \bmod p \iff \ell(a) \mid ek \iff \lambda \mid ek \iff \frac{\lambda}{\mathrm{GCD}(e, \lambda)} \mid k$$

The only unjustified statement is the final statement, so let's prove that.

> Let $d = \mathrm{GCD}(e, \lambda)$.
>
> ($\Rightarrow$) By Bézout's Identity $d = ex + \lambda y$ for some integers x, y. Therefore $dk = ekx + \lambda ky$. Since $\lambda \mid ek$ and clearly $\lambda \mid \lambda k$, hence $\lambda \mid (ekx + \lambda ky) = dk$ and thus $(\lambda/d) \mid k$.
>
> ($\Leftarrow$) Since $d \mid e$, therefore $dk \mid ek$. By assumption $(\lambda/d) \mid k$, hence $\lambda \mid dk$. By transitivity of divisibility, we obtain $\lambda \mid ek$.

Therefore, since $\ell(a^e)$ is the minimum such k, necessarily $\ell(a^e) = \lambda / \mathrm{GCD}(e, \lambda)$.

Hence, $\ell(a^e) = \lambda$ if and only if $\mathrm{GCD}(e, \lambda) = 1$. Thus,

$$\begin{aligned}\#\Phi_\lambda(p) &= \#\{a^e \ : \ 0 \leqslant e < \lambda \text{ and } \mathrm{GCD}(e, \lambda) = 1\} \\ &= \#\{e \ : \ 0 \leqslant e < \lambda \text{ and } \mathrm{GCD}(e, \lambda) = 1\} \\ &= \#\Phi(\lambda) \\ &= \varphi(\lambda)\end{aligned}$$

□

Theorem 14.4 (Gauss)**.** *Let p be prime. Then there are exactly $\varphi(p-1)$-many primitive roots in $\Phi(p)$. Recall that primitive roots are those $a \in \Phi(p)$ such that $\ell(a) = p-1$.*

Proof. Since $\ell(a) \cdot c(a) = p-1$, for any $a \in \Phi(p)$, we have $\ell(a) \mid (p-1)$. Furthermore, note that $\ell(a) > 0$; hence $\ell(a) \in \mathscr{D}(p-1)$ for any a.

Now, for each $\lambda \in \mathscr{D}(p-1)$, the previous Lemma tells us that

$$\Phi_\lambda(p) = \{a \in \Phi(p) \ : \ \ell(a) = \lambda\}$$

has either 0 or $\varphi(\lambda)$-many elements. Our aim is to prove that for any such λ, we always have $\Phi_\lambda(p) \neq \varnothing$, and then the result will follow by looking at $\lambda = p-1$, since $\Phi_{p-1}(p)$ is exactly the set of primitive roots.

Note for $\lambda_1 \neq \lambda_2$, necessarily $\Phi_{\lambda_1}(p) \cap \Phi_{\lambda_2}(p) = \varnothing$. Therefore, $\Phi(p) = \coprod_{\lambda \in \mathscr{D}(p-1)} \Phi_\lambda(p)$. Hence,

$$p - 1 = \#\Phi(p) = \sum_{\lambda \in \mathscr{D}(p-1)} \#\Phi_\lambda(p) = \sum_{\lambda \in \mathscr{D}(p-1)} \begin{cases} 0 & \text{(or)} \\ \varphi(\lambda) \end{cases}$$

Now, by Lemma 12.1, 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 $\Phi_{\lambda_0}(p) = \varnothing$, i.e. $\#\Phi_{\lambda_0}(p) = 0$. Then

$$\sum_{\lambda \in \mathscr{D}(p-1)} \varphi(\lambda) = p - 1 = \#\Phi(p) = \sum_{\lambda \in \mathscr{D}(p-1)} \#\Phi_\lambda(p) = \sum_{\lambda \in \mathscr{D}(p-1) \setminus \{\lambda_0\}} \#\Phi_\lambda(p) < \sum_{\lambda \in \mathscr{D}(p-1)} \varphi(\lambda);$$

giving us a contradiction.

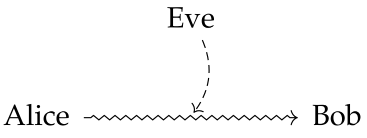
Thus, $\Phi_\lambda(p) \neq \varnothing$, for all $\lambda \in \mathscr{D}(p-1)$. In particular, $\Phi_{p-1}(p) \neq \varnothing$, and therefore

$$\#\Phi_{p-1}(p) = \varphi(p-1).$$

We have concluded more, not only did we prove that there exist primitive roots and there are $\varphi(p-1)$ of them, but also that there are numbers in $\Phi(p)$ that achieve every possible length λ (necessarily a positive divisor of $p-1$) and that there are $\varphi(\lambda)$-many of them. □

An Application of Gauss' Theorem on Primitive Roots (Theorem 14.4).

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 mod $p-1$ (*private key*) and computes $A := g^a$ mod p and send it to Bob.

Bob chooses b mod $p-1$ (*private key*) and computes $B := g^b$ mod p and sends it to Alice.

$$\begin{tikzcd}
\text{Alice} \arrow[r, squiggly, bend left, "A"] & \text{Bob} \arrow[l, squiggly, bend left, "B"]
\end{tikzcd}$$

(3) Alice computes B^a mod p and Bob computes A^b mod p, both are $\equiv g^{ab}$ mod 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 $A \equiv g^a$ mod p is difficult. This is the *discrete logarithm problem*.

14.1. Problems

Problem 14.1. Let $a \in \Phi(m)$ for a modulus m, and define $\ell(a)$ to be the smallest positive integer such that

$$a^{\ell(a)} \equiv 1 \text{ mod } m;$$

that is, $\ell(a)$ is the length of the cycles in the multiplicative modular dynamics given by

$$\boxed{\times a \text{ mod } m} : \Phi(m) \to \Phi(m).$$

We have already seen that $\ell(a) \mid \varphi(m)$.

(a) Prove that if e is any integer such that $a^e \equiv 1$ mod m, then $\ell(a) \mid e$.
Hint: use the division algorithm with respect to e and $\ell(a)$ arriving at a contradiction to the minimality of $\ell(a)$.

(b) Suppose p is an odd prime and q is a prime factor of $2^p - 1$. Prove that $q \equiv 1$ mod $2p$.

Problem 14.2. Find the smallest positive integer a such that $2^a \equiv 11$ mod p, for the two primes: $p = 23$ and $p = 37$.

Problem 14.3. Find Alice and Bob's secret number S, if $g = 3,\ p = 17,\ A = 8$ and $B = 7$.

15. Lecture 15 (11/16)

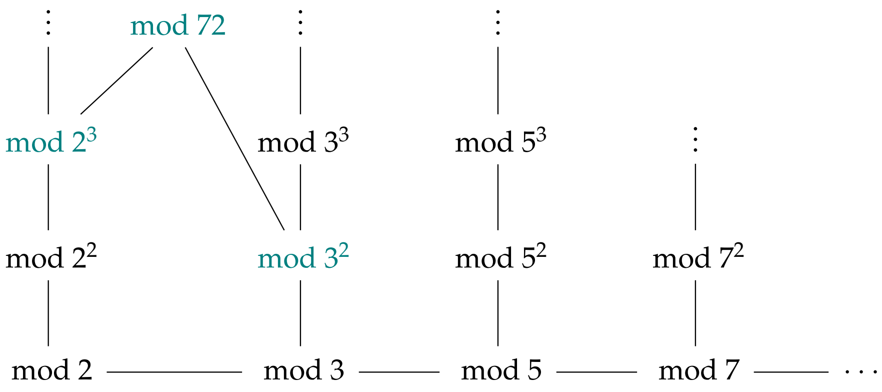
Assembling the Modular World

Back to the motivation of modular arithmetic

e.g. (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 3s, then 2 oranges are left.

If I group them in 5s, then 3 oranges are left.

If I group them in 7s, then 2 oranges are left.

How many oranges are there in total?

Translation of the Question. 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?

Notation (non-standard). Let d, e be moduli and a, b are integers. For any integer x, we write

$$x \equiv [a, b] \bmod [d, e], \quad \text{if } \ x \equiv a \bmod d \ \text{ and } \ x \equiv b \bmod e$$

e.g. Let $d = 3$, $e = 5$, then $67 \equiv [1, 2] \bmod [3, 5]$

Theorem 15.1 (Chinese Remainder Theorem, CRT)**.** *Let d and e be moduli. Assume that d and e are coprime, that is* $\mathrm{GCD}(d,e)=1$*. Then there's a one-to-one correspondence*

$$\left\{ (a,b) \in \mathbb{Z}^2 \;\middle|\; \begin{array}{l} 0 \leqslant a \leqslant d-1 \\ 0 \leqslant b \leqslant e-1 \end{array} \right\} \longleftrightarrow \{N \in \mathbb{Z} \,:\, 0 \leqslant N \leqslant de-1\}$$

in which solutions to $x \equiv [a,b] \bmod [d,e]$ *correspond to* $y \equiv N \bmod de$*.*

e.g. We want to assemble the congruences

$$N \equiv [6,2] \text{ mod } [7,5]$$

(1) Write each of the two congruences into integer equations

$$N \equiv 6 \text{ mod } 7, \quad \text{if and only if} \quad N = 6+7x, \text{ for some integer } x$$

$$N \equiv 2 \text{ mod } 5, \quad \text{if and only if} \quad N = 2+5y, \text{ for some integer } y$$

(2) Combine the two equations into one.

$$6+7x = N = 2+5y$$

$$7x-5y=-4$$

(3) Find *one* particular solution using the division algorithm

$$\begin{aligned} 7 &= 5\cdot 1+2 & \qquad 1 &= 5-2\cdot 2 \\ 5 &= 2\cdot 2+1 & &= 5-2(7-5) \\ 2 &= 1\cdot 2+0 & &= 7(-2)+5(3) \end{aligned}$$

So, we have

$$-4 = -4\cdot 1 = -4(7(-2)+5(3)) = 7(8)-5(12).$$

Therefore $(x,y)=(8,12)$.

(4) Return to N. Our computations give us

$$N = 7(8)+6 = 62$$

is a solution to $N \equiv [6,2]$ mod $[7,5]$.

The Chinese Remainder Theorem tells us that $N=62$ is unique upto mod $7\cdot 5$. That is, if M is another solution to $N \equiv [6,2]$ mod $[7,5]$, then $M \equiv 62$ mod $35 \equiv 27$ mod 35.

Proof of Theorem 15.1 (CRT). Let's start by defining the sets under consideration

$$C_d = \{a \in \mathbb{Z} \,:\, 0 \leqslant a \leqslant d-1\}$$

$$R_e = \{b \in \mathbb{Z} \,:\, 0 \leqslant b \leqslant e-1\}$$

$$P_{de} = \{N \in \mathbb{Z} \,:\, 0 \leqslant N \leqslant de-1\}$$

and consider the function defined as

$$f : P_{de} \to C_d \times R_e, \;\; N \mapsto (a_N, b_N),$$

where

$a_N :=$ natural representative of N modulo d, i.e., the remainder in division of N by d;

$b_N :=$ natural representative of N modulo e, i.e., the remainder in division of N by e.

In particular, $a_N \equiv N \bmod d$ and $b_N \equiv N \bmod e$.

Injectivity of f. Say M, N are such that they get mapped to the same element under f, say (a, b). Then

$$\begin{aligned} M &\equiv [a, b] \bmod [d, e] \\ N &\equiv [a, b] \bmod [d, e] \\ \text{So, } \; M - N &\equiv [0, 0] \bmod [d, e] \end{aligned}$$

That is, $d \mid (M - N)$ and $e \mid (M - N)$. Since d and e are coprime, we have

$$de \mid (M - N)$$

Hence, $M - N = 0$ or $|M - N| \geqslant de$. Now, since $M, N \in P_{de}$, we have $0 \leqslant M, N \leqslant de - 1$ since $M, N \in P_{de}$, 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 of f. Note that $|P_{de}| = de$ and $|C_d \times R_e| = |C_d| \cdot |R_e| = de$. That is, f is an injective map between two sets of the same size. Therefore, f is a bijection. □

Remark 15.2. The interpretation that we will use in practice is the following:

Given moduli d and e such that $\mathrm{GCD}(d, e) = 1$, then

$$x \equiv N \bmod de \quad \text{if and only if} \quad x \equiv [N, N] \bmod [d, e]$$

Remark 15.3. One can use Theorem 15.1 to give another proof of the formula of the Euler totient function. One can, first, directly show that $\varphi(p^e) = p^{e-1}(p - 1)$. Then, one shows that the one-to-one correspondence f in Theorem 15.1 restricts to a one-to-one correspondence

$$\Phi(de) \to \Phi(d) \times \Phi(e)$$

Taking cardinalities, we obtain $\varphi(de) = \varphi(d)\varphi(e)$, whenever $\mathrm{GCD}(d, e) = 1$. This shows that φ is multiplicative.

Combining these two facts gives us the formula seen in Theorem 11.6.

The real reason for all of this works is because the bijection f in Theorem 15.1, when $\mathrm{GCD}(d, e) = 1$, was in fact a *ring isomorphism* given as

$$\begin{aligned} &f : \mathbb{Z}/de\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}; \\ &N \bmod de \mapsto (N \bmod d, N \bmod e) \end{aligned}$$

Applications of the Chinese Remainder Theorem.

I. *More then two congruences.* Recall the ancient riddle: find the positive integer $N \leqslant 100$ such that

$$N \equiv 2 \bmod 3 \tag{1}$$
$$N \equiv 2 \bmod 7 \tag{2}$$
$$N \equiv 3 \bmod 5 \tag{3}$$

Solution. From (1) and (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, (1) and (2) give us

$$N \equiv 2 \bmod 21 \tag{4}$$

We solve the simultaneous congruence given by (3) and (4). We rewrite them as

$$N = 3 + 5x, \quad N = 2 + 21y$$

for some integers x, y. Therefore $3 + 5x = N = 2 + 21y$, 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, the Chinese Remainder Theorem 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, $2^2, \ldots, 34^2$ mod 35 and see if any one of them is $\equiv 29$ mod 35.

A better method: break $x^2 \equiv 29 \bmod 35$ into two congruences;

$$\begin{cases} x^2 \equiv 29 \bmod 5 \equiv 4 \bmod 5 & (\underline{5}) \\ x^2 \equiv 29 \bmod 7 \equiv 1 \bmod 7 & (\underline{7}) \end{cases}$$

Since 5 and 7 are primes, we can use polynomial methods, i.e.

$$\begin{aligned} (\underline{5}) \iff x^2 - \overline{4} = 0 &\iff (x - \overline{2})(x + \overline{2}) = \overline{0} \\ &\iff x = \overline{2} \ \text{ or } \ x = -\overline{2} = \overline{3} \\ &\iff x \equiv 2 \bmod 5 \ \text{ or } \ x \equiv -2 \bmod 5 \end{aligned}$$

$$\begin{aligned} (\underline{7}) \iff x^2 - \overline{1} = 0 &\iff (x - \overline{1})(x + \overline{1}) = \overline{0} \\ &\iff x = \overline{1} \ \text{ or } \ x = -\overline{1} = \overline{6} \\ &\iff x \equiv 1 \bmod 7 \ \text{ or } \ x \equiv -1 \bmod 7 \end{aligned}$$

Therefore, we have four possibilities

	$x \equiv 1 \bmod 7$	$x \equiv 6 \bmod 7$
$x \equiv 2 \bmod 5$	$\bullet_1$	$\bullet_2$
$x \equiv 3 \bmod 5$	$\bullet_3$	$\bullet_4$

e.g. Let's consider $\bullet_1$, that is $x \equiv 1 \bmod 7$ and $x \equiv 2 \bmod 5$. Rewrite as

$$x = 1 + 7a \quad \text{and} \quad x = 2 + 5b$$

for some integer a, b. Then

$$7a - 5b = 1$$

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, and we get our answer

	$x \equiv 1 \bmod 7$	$x \equiv 6 \bmod 7$
$x \equiv 2 \bmod 5$	$x \equiv 22 \bmod 35$	$x \equiv 27 \bmod 35$
$x \equiv 3 \bmod 5$	$x \equiv 8 \bmod 35$	$x \equiv 13 \bmod 35$

That is, $x = 8$, 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

$$x^2 \equiv 6 \bmod 35$$

Yes, we have a solution

$$\underset{\text{CRT}}{\iff} \begin{cases} x^2 \equiv 6 \bmod 5 \\ x^2 \equiv 6 \bmod 7 \end{cases}$$

$$\iff \begin{cases} x^2 \equiv 1 \bmod 5 \\ x^2 \equiv 6 \bmod 7 \end{cases}$$

$$\iff \begin{cases} x \equiv 1 \bmod 5 \;\text{ or }\; x \equiv -1 \bmod 5 \\ \textit{never happens} \end{cases}$$

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 have $x^2 \equiv 6 \bmod 35$.

Quadratic Residues

Definition 15.4. 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. Therefore, one can interpret this as a method to test for irreducibilities of quadratic polynomials modulo p.

e.g. Let $p = 11$,

x mod 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 mod 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 $\mathbb{F}_{11} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{10}\}$, the quadratic residues are

$$\overline{0}, \overline{1}, \overline{4}, \overline{9}, \overline{5}, \overline{3}$$

and the quadratic non-residues are

$$\overline{2}, \overline{6}, \overline{7}, \overline{8}, \overline{10}.$$

Hence, in $\Phi(11) = \{1, 2, \dots, 10\}$, we have *five* quadratic residues and *five* quadratic non-residues.

Our 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?

15.1. Problems

Problem 15.1. 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 15.2 (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 $\Phi(5^8)$.

Problem 15.3. 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 p^{-e}. For example,

$$|20|_2 = \frac{1}{4}, \quad |20|_3 = 1, \quad |20|_5 = \frac{1}{5}$$

We define $|0|_p := 0$. 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 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

$$B(a, p^{-e}) := \{x \in \mathbb{Z} \;:\; |x-a|_p < p^{-e}\}$$

using the language of congruences, where $e \geqslant 0$ is also an integer.

Problem 15.4. We extend Problem 15.3 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 above problem, the *p-adic norm* of an integer x, denoted $|x|_p$, is defined to be p^{-e}. For example,

$$\left|\frac{42}{40}\right|_2 = 4, \quad \left|\frac{42}{40}\right|_3 = \frac{1}{3}, \quad \left|\frac{42}{40}\right|_5 = 5, \quad \left|\frac{42}{40}\right|_7 = \frac{1}{7}$$

We define $|0|_p := 0$ as above, and the *p-adic distance* is similarly defined.

(a) As in the previous problem, prove that $|-x|_p = |x|_p\,,\ |xy|_p = |x|_p\,|y|_p$, and the ultrametric triangle inequality $|x+y|_p \leqslant \max\{|x|_p\,, |y|_p\}$. As before, this inequality 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 get xy and $x + y \in S$.

(Since, clearly $0, 1 \in S$, we have actually proven that S is a ring.)

(c) We can explicitly describe S. Prove that

$$S = \left\{\frac{a}{b} \in \mathbb{Q} \;:\; a, b \in \mathbb{Z},\ p \nmid b\right\}, \quad \frac{a}{b} \text{ is understood to be reduced}$$

Problem 15.5. 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.

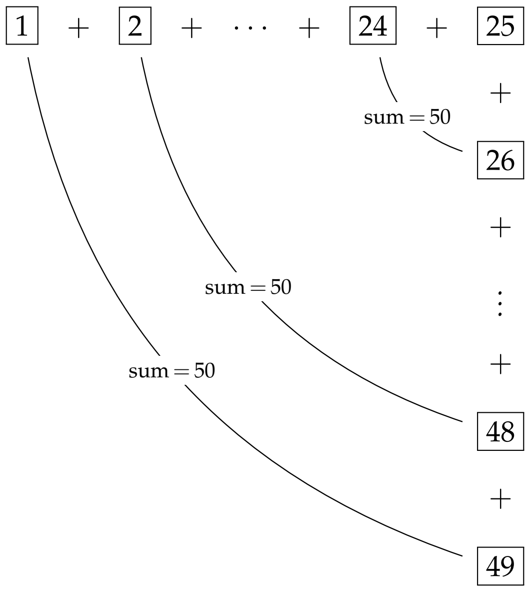
(c) By combining (a) and (b) and then applying the Chinese Remainder Theorem, solve the congruence $x^2 \equiv 17 \bmod 208$; more precisely, find $0 \leqslant x < 208$ that solves the given congruence.

Note that $208 = 13 \cdot 16$ and $\mathrm{GCD}(13, 16) = 1$.

16. Lecture 16 (11/18)

Ideas of Partnership.

Example 16.1 (additive)**.** *Compute* $1 + 2 + 3 + \cdots + 49$.



Therefore,

$$\text{Sum} = 50 \cdot (\#\,\textit{pairs}) + 25 = 50 \cdot 24 + 25 = 1200 + 25 = 1225$$

Theorem 16.2 (Wilson)**.** *Let p be a prime number. Then we have*

$$(p-1)! \equiv -1 \; \textit{mod } p$$

Proof. Consider $\Phi(p) = \{1, 2, \ldots, p-1\}$,

Partner $x \in \Phi(p)$ with $y \in \Phi(p)$ if and only if $xy \equiv 1 \bmod p$. That is, partner x with its multiplicative inverse y modulo p.

Know: any $x \in \Phi(p)$ has a unique multiplicative modulo p in $\Phi(p)$.

Question. When is $x \in \Phi(p)$ its own partner?

Answer. It is

$$\begin{aligned} \iff x \cdot x \equiv 1 \bmod p \iff & \; x^2 - 1 \equiv 0 \bmod p \\ \iff & \; x^2 - \overline{1} = \overline{0}, \text{ in } \mathbb{F}_p \\ \iff & \; (x - \overline{1})(x + \overline{1}) = \overline{0}, \text{ in } \mathbb{F}_p \\ \iff & \; x = -\overline{1} \text{ or } x = \overline{1}, \text{ in } \mathbb{F}_p \\ \iff & \; x \equiv -1 \equiv p - 1 \bmod p \text{ or } x \equiv 1 \bmod p \end{aligned}$$

$(p = 2)$ A special case

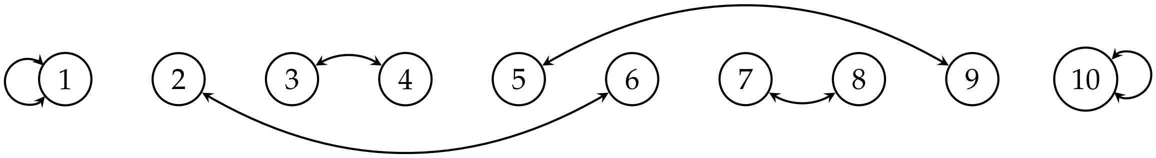
$$(p-1)! = (2-1)! = 1! = 1 \equiv -1 \bmod 2$$

$(p \geqslant 3)$ $\Phi(p)$ contains two distinct elements, namely 1 and $p-1$, that don't get partnered with different elements. All the other elements x get partnered with some $y \neq x$. Therefore

$$\begin{aligned}(p-1)! &= \text{the product of all elements in } \Phi(p). \\ &= 1 \cdot (p-1) \cdot (\text{partnered products}) \\ &\equiv (p-1) \cdot 1 \bmod p \\ &\equiv -1 \bmod p\end{aligned}$$

□

e.g. Let $p = 11$, the partnership specified in the proof above is



Proposition 16.3. *Let p be an odd prime, so $\#\Phi(p) = p-1$ is even. Then, exactly half* $(= (p-1)/2)$ *of* $\Phi(p)$ *are quadratic residues, the other half quadratic non-residues.*

Proof. If $x \in \Phi(p)$, then $p \nmid x^2$, so we have a function

$$\Phi(p) \xrightarrow{f} \Phi(p),\ x \mapsto x^2 \bmod p$$

Note that $x^2 \bmod p$ here refers to the natural representative of x^2 modulo p in $\Phi(p)$.

Let R be the image of f. By definition, R is the set of quadratic residues in $\Phi(p)$.

> **Claim.** The function $\Phi(p) \xrightarrow{f} R$ is a two-to-one function. That is, for any $a \in R$, there exist exactly two $x_1, x_2 \in \Phi(p)$ such that $f(x_1) = a = f(x_2)$. Equivalently, $\#f^{-1}(a) = 2$.
>
> *Proof of Claim.* Consider the polynomial $r(T) = T^2 - \overline{a}$, for any $a \in R$, and let $y \in f^{-1}(a)$. Then $a = f(y)$, i.e. $y^2 \equiv a \bmod p$, or equivalently $r(\overline{y}) = 0$. Therefore, $f^{-1}(a)$ consists of roots of $r(T)$.
>
> By definition of R, there's atleast one $x_1 \in \Phi(p)$ such that $a = f(x_1)$, i.e. $x_1^2 \equiv a \bmod p$, or equivalently $r(\overline{x}_1) = 0$. Now, $x_2 = p - x_1 \in \Phi(p)$ 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, note that $x_1 \neq x_2$ as one is odd and the other even, 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, $\#R = \dfrac{\#\Phi(p)}{2} = \dfrac{p-1}{2}$. □

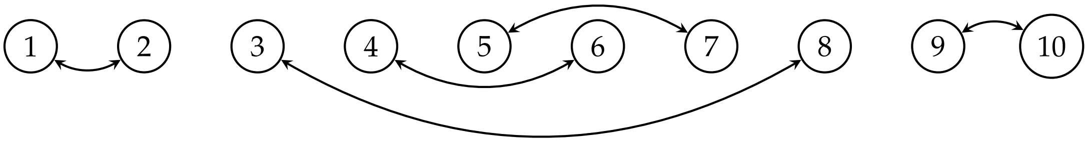
Definition 16.4. Let p be a prime number and $a, x, y \in \Phi(p)$. Say that x and y are a-partners if

$$xy \equiv a \bmod p$$

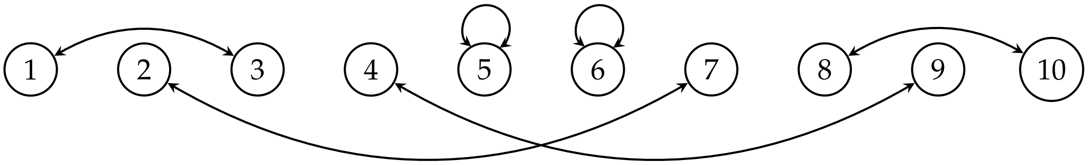
e.g. Let $p = 11$,

$a = 1$, this 1-partnership is what we used in the proof of Theorem 16.2.

$a = 2$,



$a = 3$,



Remark 16.5. We note that every $x \in \Phi(p)$ has an a-partner. This is because any such x has a multiplicative inverse z modulo p, that is $xz \equiv 1 \bmod p$. Then taking $y \in \Phi(p)$ to be such that $y \equiv az \bmod p$ (that is, y is the natural representative of az modulo p) we have

$$xy \equiv a(xz) \equiv a \bmod p$$

Hence y is an a-partner of x.

Theorem 16.6 (Euler). *Let p be an odd prime, and let $a \in \Phi(p)$. 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 Theorem 11.2 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's *no* $x \in \Phi(p)$ 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 $x \in \Phi(p)$ has an a-partner $y \in \Phi(p)$, necessarily with $y \neq x$. Hence, by Corollary 16.2, we have

$$\begin{aligned} -1 &\equiv (p-1)! \bmod p \\ &\equiv (\text{product of elements in } \Phi(p)) \bmod p \\ &\equiv a^{\frac{p-1}{2}} \bmod p \end{aligned}$$

($\Rightarrow$) 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 $x \in \Phi(p)$ 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 Corollary 11.2. Thus, necessarily, a is a QNR. □

Remark 16.7. Note that if $a \in \Phi(p)$ is a primitive root modulo p, then it's necessarily a quadratic non-residue. Since, by definition, $p-1$ is the smallest positive integer such that $a^{p-1} \equiv 1 \bmod p$. Therefore, necessarily, $a^{\frac{p-1}{2}} \not\equiv 1 \bmod p$. Hence, a is a QNR.

Example 16.8. *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,

$$\begin{aligned} 3^1 &\equiv 3 \bmod 43 \\ 3^2 &\equiv 9 \bmod 43 \\ 3^4 &\equiv 81 \equiv -5 \bmod 43 \\ 3^{16} &\equiv (-5)^4 \equiv 125 \cdot 5 \equiv (-4) \cdot 5 \equiv -20 \bmod 43 \end{aligned}$$

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 16.9 (in-class)**.** *Determine whether $a = 2$ is a quadratic residue modulo $p = 29$.*

Corollary 16.10. *Let p be an odd prime. Then*

$$-1 \textit{ is a quadratic residue mod } p \textit{ if and if } p \equiv 1 \textit{ mod } 4$$

Equivalently, $T^2 + \overline{1} \in \mathbb{F}_p[T]$ is reducible if and only if $p \equiv 1$ mod 4.

Proof. By Theorem 16.6, -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 $p \equiv 1$ mod 4. □

16.1. Problems

Problem 16.1. Let p be an odd prime. Recall that a primitive root modulo p is an integer g such that

$$g^{p-1} \equiv 1 \bmod p$$

and for no $0 < e < p - 1$ do we have $g^e \not\equiv 1$ mod p. The results that we proved in this lecture can be proved via the existence of g (Theorem 14.4).

(a) Consider $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{\overline{0}\}$ and let g be a primitive root. Prove that

$$\mathbb{F}_p^\times = \{\overline{g}^e \ : \ 0 \leqslant e < p-1\}$$

(b) Use a primitive root g to demonstrate that -1 is a QR modulo p if and only if $p \equiv 1$ mod 4.

(c) Use a primitive root g to prove Theorem 16.2, by first showing that

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

(d) Given a primitive root g, and an integer a such that $a \equiv 0 \bmod p$, prove that a is a QR modulo p if and only if $a \equiv g^e \bmod p$ for an even number e. Use this to prove Theorem 16.6.

17. Lecture 17 (11/23)

Remark 17.1. Suppose p is a prime such that $p \equiv 1 \bmod 4$, 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, $A^2 \equiv AB \equiv -1 \bmod p$.

e.g. Let $p = 13$, then $A = 1 \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot 11 \equiv 8 \bmod 13$. Then $x = 8$ is such that

$$x^2 = 64 \equiv -1 \bmod 13.$$

The other being $y = 13 - 8 = 5$.

Definition 17.2. Let p be a prime number, and a an integer. Then we define the *Legendre symbol* by the rule

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

Important Observation. If $a \equiv b \bmod p$, then

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

We rephrase Corollary 16.10 as follows

Corollary 17.3 (First Quadratic Reciprocity Law)**.** *Let p be an odd prime. Then*

$$\left(\frac{1}{p}\right) = 1, \quad \textit{for any } p$$

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

e.g.

- $\left(\frac{3}{43}\right) = -1$, 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 16.6 using the Legendre symbol.

Theorem 17.4 (Euler)**.** *Let p be an odd prime, and a an integer. Then,*

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

Note that $1 \not\equiv -1$ *mod p for odd primes.*

One non-trivial consequence of Theorem 17.4.

Corollary 17.5. *Let p be an odd prime, and let a, b be integers. Then*

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

(the Legendre symbol is completely multiplicative). That is, ab is a QR modulo p

$$\iff \begin{cases} \textit{either } \text{both } \textit{a and b are QR's} & \textit{(or)} \\ \textit{either } \text{both } \textit{a and b are QNR's} \end{cases}$$

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 17.4, we have

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

But necessarily, both LHS and RHS are ±1. Since p is an odd prime, $1 \not\equiv -1$ mod p, therefore we can replace $\equiv$ with $=$ above. Thus,

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

□

e.g. $p = 13$, $a = 2$, $b = 6$. Note,

$$2^{\frac{13-1}{2}} = 2^6 = 64 \equiv -1 \bmod 13;$$

$$\text{so, } \left(\frac{2}{13}\right) = -1$$

$$\begin{aligned} 6^{\frac{13-1}{2}} = 6^6 = (6^2)^3 = 36^3 &\equiv (-3)^3 \bmod 13 \\ &\equiv -27 \bmod 13 \\ &\equiv -1 \bmod 13; \end{aligned}$$

$$\text{so, } \left(\frac{6}{13}\right) = -1$$

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 17.6 (Second Quadratic Reciprocity Law)**.** *Let p be a prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 0 & \text{if } p = 2 \\ 1 & \text{if } p \equiv \pm 1 \text{ mod } 8 \\ -1 & \text{if } p \equiv \pm 3 \text{ mod } 8 \end{cases}$$

Proof. We first note that 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 $(p-1)!$

$$A = 1 \cdot 2 \cdot 3 \cdots \frac{p-3}{2} \cdot \frac{p-1}{2}$$

$$B = 2 \cdot 4 \cdot 6 \cdots (p-3) \cdot (p-1)$$

$$C = 1 \cdot 3 \cdot 5 \cdots (p-4) \cdot (p-2)$$

There are three relations among A, B and C mod 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 summarise

$$B = 2^{\frac{p-1}{2}} A \tag{1}$$

$$2^{\frac{p-1}{2}} \equiv BD \bmod p \tag{1'}$$

$$B \equiv (-1)^{\frac{p-1}{2}} C \bmod p \tag{2}$$

$$C \equiv (-1)^{\left\lfloor \frac{p-1}{4} \right\rfloor} A \bmod p \tag{3}$$

$$(-1)^{\left\lfloor \frac{p-1}{4} \right\rfloor} \equiv CD \bmod p \tag{3'}$$

Therefore, by Theorem 17.4

$$\begin{aligned} \left(\frac{2}{p}\right) &\equiv 2^{\frac{p-1}{2}} \bmod p \\ &\underset{(1')}{\equiv} BD \bmod p \\ &\underset{(2)}{\equiv} (-1)^{\frac{p-1}{2}} CD \bmod p \\ &\underset{(3')}{\equiv} (-1)^{\frac{p-1}{2}} (-1)^{\left\lfloor \frac{p-1}{4} \right\rfloor} \bmod p \end{aligned}$$

There are four possibilities of odd primes p modulo 8, $p \equiv 1$, 3, 5 or 7 mod 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

□

e.g. Consider $p = 10337,\ p = 10337 \equiv 337 \equiv 17 \equiv 1 \bmod 8$. Therefore

$$\left(\frac{2}{10337}\right) = 1$$

Theorem 17.7 (Gauss, Third Quadratic Reciprocity Law)**.** *Let p and q be odd primes. Then*

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

Equivalently,

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

That is, there's a tangible relation between the irreducibility of $T^2 - \overline{p} \in \mathbb{F}_q[T]$ and $T^2 - \overline{q} \in \mathbb{F}_p[T]$

Application. Very effective way to compute $\left(\frac{a}{p}\right)$.

Question. Is $a = 3$ a quadratic residue modulo $p = 73$? That is, is the polynomial $T^2 - \overline{3} \in \mathbb{F}_{73}[T]$ irreducible?

Answer. We can employ three methods

- (Brute Force) Compute x^2 mod 73 for $x = 1, \ldots, 72$ and see if $a = 3$ appears in the list. For a large primes ($p \sim 2^{4000}$) this is inefficient.
- (Euler's Theorem) Compute $3^{\frac{73-1}{2}}$ mod 73. Effective for computers.
- (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 17.8 (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) If q is an odd prime $\neq p$

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

Example 17.9. *Consider the polynomial $f(T) = T^2 - \overline{12}T + \overline{7} \in \mathbb{F}_p[T]$. For what primes p is $f(T)$ irreducible?*

Answer. First note that if $p = 2$, $f(T) = T^2 - \overline{12}T + \overline{7} = T^2 + \overline{1} = (T + \overline{1})^2$. Therefore $f(T)$ is reducible for $p = 2$.
Now, assume that p is odd. Note that

$$\begin{aligned} f(T) = T^2 - \overline{12}T + \overline{7} &= T^2 - \overline{2} \cdot \overline{6}T + \overline{36} - \overline{29} \\ &= (T - \overline{6})^2 - \overline{29} \end{aligned}$$

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 $(a - \overline{6})^2 - \overline{29} = \overline{0}$ for some $a \in \mathbb{F}_p$ if and only if $\overline{29}$ is a square modulo p if and only if 29 is a QR modulo p.

Hence, by Problem 13.1 and looking at the contrapositive, we have that $f(T)$ is irreducible if and only if 29 is a QNR modulo p if and only if

$$\left(\frac{29}{p}\right) = -1$$

By Quadratic Reciprocity, note that

$$\left(\frac{p}{29}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{29-1}{2}\right)}\left(\frac{29}{p}\right) = (-1)^{(p-1)\cdot 7}\left(\frac{29}{p}\right) = \left(\frac{29}{p}\right)$$

since p is an odd prime.

Thus $f(T)$ is irreducible if and only if

$$\left(\frac{p}{29}\right) = -1$$

Since 29 is a prime, we have $p \equiv m \bmod 29$ for $1 \leqslant m \leqslant 28$. Checking for what such m we get

$$\left(\frac{m}{29}\right) = -1$$

gives us our answer. □

17.1. Problems

Problem 17.1. Consider the polynomial $f(T) = T^2 - \overline{6}T + \overline{4} \in \mathbb{F}_p[T]$, where p is a prime. In this problem, we will determine the primes for which $f(T)$ is irreducible.

(a) "Completing the square", rewrite f as $(T - \overline{a})^2 - \overline{q}$ 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 what p mod q possibly can be and other Quadratic Reciprocity Laws.

(d) Conclude. Your answer should look something like

$$f(T) \text{ is irreducible if and only if } p \equiv \underline{\quad} \bmod q.$$

Problem 17.2. 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

$$\left(\frac{a}{n}\right) := \left(\frac{a}{3}\right)^{e_3} \cdot \left(\frac{a}{5}\right)^{e_5} \cdot \left(\frac{a}{7}\right)^{e_7} \cdots$$

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) $\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{GCD}(a,n) \neq 1 \\ \pm 1 & \text{GCD}(a,n) = 1 \end{cases}$.

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

(f) If a is a quadratic residue modulo n and $\text{GCD}(a,n) = 1$, then $\left(\frac{a}{n}\right) = 1$.

Unlike the Legendre symbol, if $\left(\frac{a}{n}\right) = 1$ then a may not be a quadratic residue modulo n.

18. Lecture 18 (11/30)

Example 18.1. *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 the prime $p > 3$ and then Quadratic Reciprocity gives us

$$\begin{aligned}\left(\frac{3}{p}\right) &= (-1)^{\left(\frac{3-1}{2}\right)\left(\frac{p-1}{2}\right)}\left(\frac{p}{3}\right)\\ &= (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)\\ &= \left(\frac{p}{3}\right)\cdot\begin{pmatrix}1 & \text{if } p \equiv 1 \bmod 4\\ -1 & \text{if } p \equiv -1 \bmod 4\end{pmatrix}\end{aligned}$$

Note that

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

Therefore

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

$$= \begin{cases}1 & \text{if } p \equiv [1,1] \bmod [3,4]\\ 1 & \text{if } p \equiv [-1,-1] \bmod [3,4]\\ -1 & \text{if } p \equiv [5,5] \bmod [3,4]\\ -1 & \text{if } p \equiv [-5,-5] \bmod [3,4]\end{cases}$$

Putting these congruences together via CRT (Remark 15.2), 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 18.2. *Does the equation*

$$x^2 = 59783y + 46, \quad 59783 = 191 \cdot 313$$

have any integer solutions?

Answer. We have the following steps

Step 1. Division algorithm is very useful for linear equations, but this is a quadratic equation.

Step 2. Reducing mod 59783, we ask if

$$x^2 \equiv 46 \bmod 59783$$

has an integer solution.

Step 3. By CRT, $x^2 \equiv 46 \bmod 59783$ has a solution if and only if

$$\begin{cases} x^2 \equiv 46 \bmod 191; \text{ and} & (1) \\ x^2 \equiv 29 \bmod 313 & (2) \end{cases}$$

have solutions.

Step 4. So, we look to see if (1) and (2) have an intger solutions, that is, compute

$$\left(\frac{46}{191}\right) \quad \text{and} \quad \left(\frac{46}{313}\right)$$

Step 5. $\left(\frac{46}{191}\right) = \left(\frac{2}{191}\right)\left(\frac{23}{191}\right)$. Note that

$$\left(\frac{2}{191}\right) = 1, \quad \text{since } 191 \equiv 7 \bmod 8$$

$$\begin{aligned} \left(\frac{23}{191}\right) &= (-1)^{\left(\frac{23-1}{2}\right)\left(\frac{191-1}{2}\right)}\left(\frac{191}{23}\right) \\ &= (-1)\left(\frac{7}{23}\right) \\ &= (-1)(-1)^{\left(\frac{7-1}{2}\right)\left(\frac{23-1}{2}\right)}\left(\frac{23}{7}\right) \\ &= (-1)^2\left(\frac{2}{7}\right) \\ &= 1 \end{aligned}$$

So, $\left(\frac{46}{191}\right) = 1 \cdot 1 = 1$. Therefore (1) has a solution.

Step 6. $\left(\frac{46}{313}\right) = \left(\frac{2}{313}\right)\left(\frac{23}{313}\right)$. Note that

$$\left(\frac{2}{313}\right) = 1, \quad \text{since } 313 \equiv 1 \text{ mod } 8$$

$$\begin{aligned}\left(\frac{23}{313}\right) &= (-1)^{\left(\frac{23-1}{2}\right)\left(\frac{313-1}{2}\right)}\left(\frac{313}{23}\right)\\ &= \left(\frac{14}{23}\right)\\ &= \left(\frac{2}{23}\right)\left(\frac{7}{23}\right)\\ &= 1(-1)\\ &= -1\end{aligned}$$

So, $\left(\frac{46}{313}\right) = -1$. Therefore (2) does not have a solution.

Hence $x^2 \equiv 46$ mod 59783 has no integer solutions. Thus

$$x^2 = 59783y + 46$$

has no integer solutions. □

An Application of the Quadratic Reciprocity Law. Fermat's Christmas Theorem

Theorem 18.3 (Fermat's Christmas Theorem)**.** *Let p be a prime such that $p \equiv 1$ mod p. Then the equation*

$$p = x^2 + y^2$$

has integer solutions. That is, p can be written as a sum of two squares.

(this appears in Fermat's letter to Mersenne dated 25th Dec, 1640)

Examples and Remarks.

- $13 = 2^2 + 3^2$ *and* $17 = 4^2 + 1^2$
- $p = 2$, $2 = 1^2 + 1^2$
- *Suppose $p \equiv 3$ mod 4. Then p cannot be written as a sum of two squares, since for integers x, y we have $x^2 + y^2 \equiv 0, 1, 2$ mod 4 as we saw some time ago.*
- *We consider the set $\mathbb{Z}[i] = \{a + bi \,:\, a, b \in \mathbb{Z}\}$, what we have then is that if $p \equiv 1$ mod 4, then $p = (x + iy)(x - iy)$ in the set $\mathbb{Z}[i]$.*

Some Geometric Preliminaries (Minkowski).

We ask a general question,

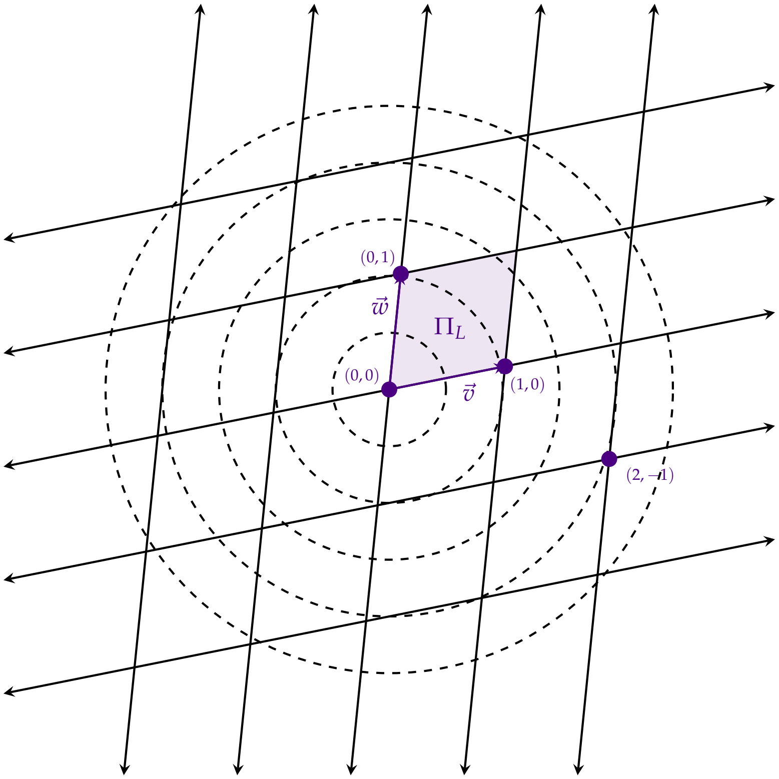
Consider a lattice (a grid of parallelograms in the plane); more precisely, fix the two non-parallel vector $\vec{v}$, $\vec{w}$ and consider

$$L = \{a\vec{v} + b\vec{w} \ : \ a, b \in \mathbb{Z}\}$$

associated is the fundamental parallelogram, given as

$$\Pi_L = \{m\vec{v} + n\vec{w} \ : \ m, n \in [0, 1]\} .$$

e.g.



Now, consider C_r's, circles of radius r centred at the origin.

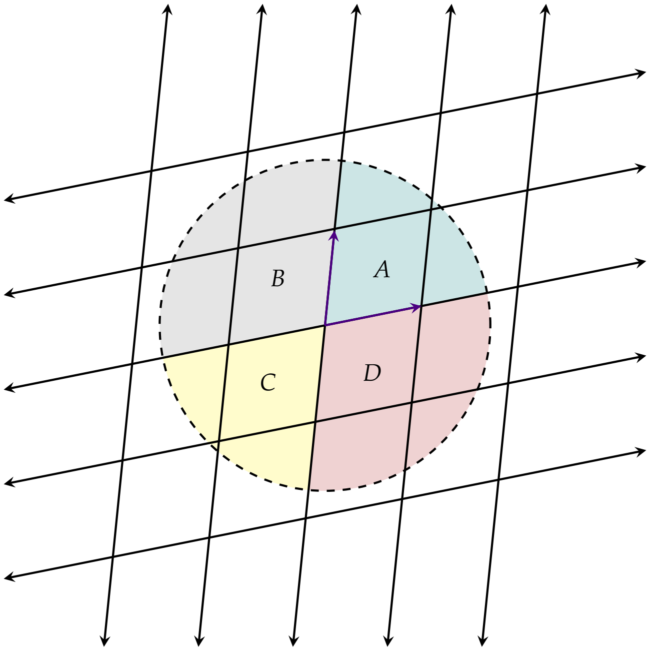
- If r is very small, the only grid point contained in the circle will be the origin.
- If r is sufficiently large, the circle will contain grid points other than the origin.

Question. When (in terms of r) can we be sure that a circle of radius r centred at the origin contains a grid point other than the origin?

A possible answer can be to take $r > \min\{|\vec{v}|, |\vec{w}|\}$; a more useful characterization, for the purposes of proving Theorem 18.3, is given as following.

Theorem 18.4 (Minkwoski)**.** *If* $\text{Area}(C_r) = \pi r^2 > 4 \cdot \text{Area}(\Pi_L)$*, then* C_r *contains at least one grid point different from the origin.*

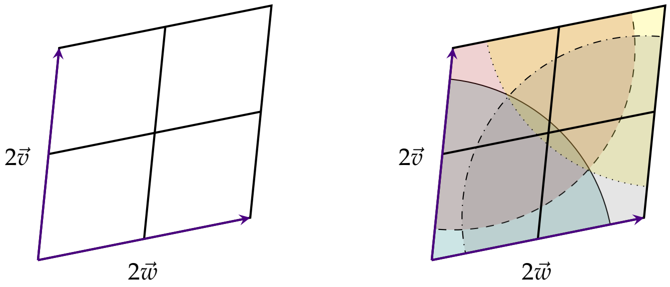
Proof. Suppose $\pi r^2 > 4 \cdot \text{Area}(\Pi_L)$. The grid divides C_r into four sectors, which we label A, B, C and D. An example is illustrated below.



Let's now do the following

- Translate the sector B by $2\vec{v}$, $\quad B + 2\vec{v} = \{\vec{b} + 2\vec{v} \ : \ \vec{b} \in B\}$
- Translate the sector D by $2\vec{w}$, $\quad D + 2\vec{w} = \{\vec{d} + 2\vec{w} \ : \ \vec{d} \in D\}$
- Translate the sector C by $2\vec{v} + 2\vec{w}$, $\quad C + 2\vec{v} + 2\vec{w} = \{\vec{c} + 2\vec{v} + 2\vec{w} \ : \ \vec{c} \in C\}$.

The straight edges of the sectors are now against the sides of the parallelogram, Π', given by $2\vec{v}$ and $2\vec{w}$.



Since $\text{Area}(\Pi') = 4 \cdot \text{Area}(\Pi_L) < \pi r^2 = \text{Area}(A) + \text{Area}(B) + \text{Area}(C) + \text{Area}(D)$, by assumption. The sectors must overlap within Π'. Illustrated above.

Therefore, atleast two of the four (translated) sectors should intersect. Hence, we have $\binom{4}{2} = 6$ possibilities.

Case I. Suppose A and $D + 2\vec{w}$ intersect. Then there exists a $P \in A$ and $Q \in D$ such that $P = Q + 2\vec{w}$. Therefore $\vec{w} = (P - Q)/2$. Since $P, Q \in C_r$ and C_r is convex, we get $\vec{w} \in C_r$.

The remaining five cases are handled similarly. □

Proof of Fermat's Christmas Theorem (Theorem 18.3). Let p be a prime such that $p \equiv 1 \bmod p$. By the First Quadratic Reciprocity Law, we know -1 is a QR modulo p. So, there exists an integer n such that $n^2 \equiv -1 \bmod p$.

Consider the set $L = \{(x, y) \in \mathbb{Z}^2 \ : \ x \equiv ny \bmod p\}$.

> **Claim.** L is a lattice. More precisely, any $(x, y) \in S$ 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 $(x, y) \in L$, then $x \equiv ny \bmod p$, i.e. $x = ny + pz$ for some integer z. Take $a = y$ and $b = z$. Then,
>
> $$a(n, 1) + b(p, 0) = y(n, 1) + z(p, 0) = (ny, y) + (pz, 0) = (ny + pz, y) = (x, y),$$
>
> as needed.
>
> 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, $(x, y) \in L$. □

Now, L is a lattice spanned by $\vec{v} = (n, 1)$ and $\vec{w} = (p, 0)$. Therefore,

$$\text{Area}(\Pi_L) = |\det(\vec{v}, \vec{w})| = \left|\det\begin{pmatrix} n & p \\ 1 & 0 \end{pmatrix}\right| = p$$

Let's consider the circle of area $4p + \varepsilon$ for some small $\varepsilon > 0$. Hence, we have considered C_r with

$$r = \sqrt{\frac{4p + \varepsilon}{\pi}}$$

By design, we have $\text{Area}(C_r) > 4 \cdot \text{Area}(\Pi_L)$, thus by Theorem 18.4 there exists an $(x, y) \in L$ with $(x, y) \neq (0, 0)$ such that it's contained in C_r. Therefore

$$0 < x^2 + y^2 < r^2 = \frac{4p + \varepsilon}{\pi}, \quad \text{since } (x, y) \in \text{interior of } C_r$$

$$x \equiv ny \bmod p, \quad \text{since } (x, y) \in L$$

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, $(x^2 + y^2)/p \in \mathbb{Z}$.

Now, note that

$$0 < \frac{x^2 + y^2}{p} < \frac{1}{p} \cdot \frac{4p + \varepsilon}{\pi} = \frac{4}{\pi} + \frac{\varepsilon}{\pi p}$$

Since our choice of ε was arbitrary, we can choose an ε, for example $\varepsilon < \pi p/2$, to get

$$\frac{4}{\pi} + \frac{\varepsilon}{\pi p} < 2$$

Thus,

$$0 < \frac{x^2 + y^2}{p} < 2$$

Necessarily, $\dfrac{x^2 + y^2}{p} = 1$, and therefore $p = x^2 + y^2$. □

Remark 18.5. Let $\Sigma_2 = \{x \in \mathbb{Z} : x = a^2 + b^2, \text{ for some } a, b \in \mathbb{Z}\}$, that is the set of integers that can be written as a sum of two squares. Theorem 18.3 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 quickly

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2;$$

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 Σ_2.

$$x \in \Sigma_2 \iff \text{every prime } q \equiv 3 \bmod 4 \text{ divides } x \text{ to an even power (take it to be 0 if } q \nmid x)$$

e.g. The integer $60 = 2^2 \cdot 3 \cdot 5$ is not a sum of two squares, since the exponent of 3 dividing it is odd.

However, $180 = 2^2 \cdot 3^2 \cdot 5$ is a sum of two squares. To find them, first write 5 as a sum of two squares: $5 = 2^2 + 1^2$. Now multiplying through by $2^2 \cdot 3^2$ we get

$$180 = 2^2 \cdot 3^2 \cdot 5 = (2 \cdot 3 \cdot 2)^2 + (2 \cdot 3 \cdot 1)^2 = 12^2 + 6^2.$$

Remark 18.6. Initiating a set-up similar to the one we had while proving Theorem 18.3, this time in $\mathbb{R}^3$, and using a version of Theorem 18.4 in three dimensions, again by Minkowski, allows us to prove the following celebrated theorem.

Theorem (Lagrange's Four-Square Theorem)**.** *Any positive integer n can be expressed as a sum of four squares. That is, there exist integers x, y, z and w such that*

$$n = x^2 + y^2 + z^2 + w^2$$

18.1. Problems

Problem 18.1. For which primes p is 5 a quadratic residue modulo p?

References

[1] Weissman, Martin H. *Illustrated Theory of Numbers*. American Mathematical Society, 2020.

[2] Jones, Gareth A. and Jones, J. Mary. *Elementary Number Theory*. Springer-Verlag London, 1998.

Number is the commanding and self-begotten container of the eternal duration of mundane concerns.

– Philolaus, as quoted by Aristotle, *Metaphysics*