Individual

Number Theory, Topology, Real and Complex Analysis

Individual Project during 2023 Summer

Note

Author:
Hyunjun Choi

July 2, 2023

Contents

1 Introduction **5**

2 Number Theory **6**
2.1 Pythagorean Triples 6
2.2 Euclidean Algorithm 7
2.3 Properties of ax + by = c 7
2.4 Congruences 8
2.5 Fermat's Little Theorem 8
2.6 Euler's Formula 9
2.7 Infinite Primes 10
2.8 kth Powers Modulo m and kth Roots Modulo m 11
2.9 Squares Modulo p 13
2.10 Study on -1 and 2 Square Modulo p 14
2.11 Quadratic Reciprocity 15
2.12 Primitive Roots and Indices 16

3 Topology **18**
3.1 Set Theory 18

List of Figures

2.1 A Unit Circle and a line passing through (-1, 0) 7

List of Tables

2.1 Table of Powers of 2 modulo m 12
2.2 Table of squares modulo 7 13
2.3 Table of solutions to $x^2 \equiv 1 \pmod{p}$ 14
2.4 Table of solutions to $x^2 \equiv 2 \pmod{p}$ and $p \pmod{8}$ 15
2.5 Table of Smallest Power of a that equals 1 Modulo 7 16
2.6 Table of Indices Modulo 13 for Base 2 16

Chapter 1

Introduction

A solid foundation in mathematics, including number theory, topology, real and complex analysis, is of paramount importance for individuals pursuing studies in natural sciences and engineering. This article is written at the request of my friend, an enthusiastic physicist and a Pleiades cluster lover, who currently is serving for obligatory military service, but wants to keep track of his study. However, I hope this article serves as a helpful resource for students, future or current researchers, and enthusiasts in various fields, including natural sciences and engineering.
Though I said that solid foundation in mathematics is important, this article is not mathematically strict. Of course I provide proofs for important theorems or features, but it omits a lot of proofs. The aim of this article is not to be a lecture note for students, but to provide intuition or serve as a cheat sheet. [Tem02]

Chapter 2

Number Theory

2.1 Pythagorean Triples

A **Primitive Pythagorean Triple (PPT)** is a tuple (a, b, c) where a, b, c have no common factors and satisfy $a^2 + b^2 = c^2$. It has few features:

Observation 2.1.1. One of a & b is odd and the other even, so c is always odd.

Observation 2.1.2. If (a, b, c) is PPT, then we can factor $a^2 = c^2 - b^2$. It looks like $c - b$ and $c + b$ are themselves always squares and have no common factors.

Proof. I first prove that $gcd(c - b, c + b) = 1$.
Let $d = gcd(c - b, c + b)$.
Then $c - b = dk$, $c + b = dl$, $k, l \in \mathbb{N}$.
Since $2b = d(l - k)$ and $2c = d(l + k)$, $d \mid gcd(2b, 2c)$.
Now suppose $gcd(b, c) = g > 1$.
Set $b = g\tilde{b}$, $c = g\tilde{c}$.
Then $a^2 = g^2(\tilde{c}^2 - \tilde{b}^2)$, which leads to $g \mid a$.
However, this is a contradiction by **Observation 2.1.1**.
Thus, $gcd(b, c) = 1$ and $gcd(2b, 2c) = 2$.
We now know that $d = 1$ or $d = 2$ as $d \mid gcd(2b, 2c)$.
If $d = 2$, then $a^2 = (c - b)(c + b) = 4kl$ so $2 \mid a$, which is again a contradiction.
Thus $d = 1$.

Now I prove $c - b$ and $c + b$ are squares.
Let $a = p_1^{n_1} \dots p_r^{n_r}$ where p_i prime, $n \in \mathbb{N}$.
Then $a^2 = p_1^{2n_1} \dots p_r^{2n_r} = (c - b)(c + b)$.
As $gcd(c - b, c + b) = 1$ by **Observation 2.1.1**, they are squares. □

A **Primitive Pythagorean Pair (PPP)** is a pair (s, t) s.t. $a = st$, $b = \dfrac{s^2 - t^2}{2}$, $c = \dfrac{s^2 + t^2}{2}$.
We can induce it by substituting $c + b = s^2$, $c - b = t^2$.

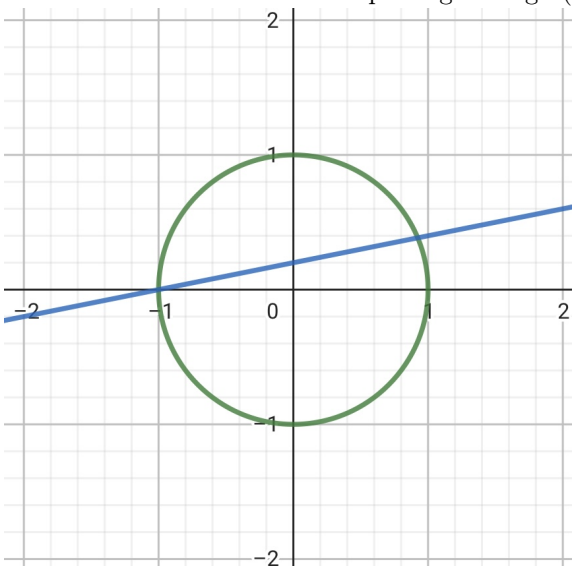
It is worth noting the relationship between the PPT and unit circle. We start by dividing the both sides of $a^2 + b^2 = c^2$ by c^2. Then we can induce the typical unit circle form by substituting as $x = \dfrac{a}{c}$ and $y = \dfrac{b}{c}$. Our goal is to find (x, y) where $x, y \in \mathbb{Q}$.

We find by exploiting geometry. As we know the trivial solution $(-1, 0)$, we draw a line that passes through $(-1, 0)$ and get the coordinate of the intersection other than $(-1, 0)$. We set the slope of the line $m \in \mathbb{Q}$ so that all the intersections are of $\mathbb{Q} \times \mathbb{Q}$.

$$x^2 + m^2(x + 1)^2 = 1(1 + m^2)x^2 + 2m^2x + (m^2 - 1) \qquad = 0(x, y) = (\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2})$$

Now let $m = \dfrac{v}{u}$ as $m \in \mathbb{Q}$. Then we can finally induce another way to describe Pythagorean triples: $(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2)$. This is equivalent form when $u = \dfrac{s + t}{2}$, $v = \dfrac{s - t}{2}$. Note that not all u, v give us PPT.

Figure 2.1: A Unit Circle and a line passing through (-1, 0)



2.2 Euclidean Algorithm

Theorem 2.2.1 (Euclidean Algorithm)**.** *Let* $r_{-1} = a$, $r_0 = b$, $r_{i-1} = q_{i+1}r_i + r_{i+1}$, $i = 0, 1, \ldots$ *until* $r_{n+1} - 0$. *Then* $r_n = gcd(a, b)$.

Proof. We inspect the last iteration: $r_{n-1} = q_{n+1}r_n + 0$.
We observe that $r_n \mid r_{n-1}$.
Now, inspect the penultimate iteration: $r_{n-1} = q_n r_{n-1} + r_n$.
We observe that $r_n \mid r_{n-2}$.
Iterating through, we get $r_n \mid r_0$ and $r_n \mid r_{-1}$.
Hence, r_n is a common divisor of a and b.
To prove that $r_n = gcd(a, b)$, suppose that $gcd(a, b) = d$.
By the definition of gcd, $d \mid a$ and $d \mid b$.
We inspect the first iteration: $a = q_1 b + r_1$.
We observe that $d \mid r_1$ Iterating through, we get $d \mid r_n$. Hence, we conclude that $d = r_n$. □

Euclidean Algorithm has some features:

Observation 2.2.1. Let $b = r_0, r_1, \ldots$ be the successive remainders in Euclidean algorithm applied to a and b. For every two steps, the remainder is reduced by at least one half: $r_{i+2} < \frac{1}{2} r_i$, $i = 0, 1, \ldots$.

Observation 2.2.2. The algorithm terminates in at most $2 \log_2 b$ steps. In particular, the number of steps is at most seven times the number of digits of b.

I omit the proofs.
Finally, I mention that $gcd(a, b) \times lcm(a, b) = ab$ and move on.

2.3 Properties of ax + by = c

Theorem 2.3.1 (Linear Equation Theorem)**.** *The equation* $ax + by = c$ *has integer solution pairs if and only if* $gcd(a, b) \mid c$. *The solution is expressible by* $(x_1 + \frac{kb}{g}, y_1 - \frac{ka}{g})$ *where* $k \in \mathbb{Z}$, (x_1, y_1) *a trivial solution.*

To prove it, apply Euclidean algorithm. I omit the specifics.

2.4 Congruences

Definition 2.4.1. a is congruent to b modulo m if $m \mid a - b$ and denote $a \equiv b \pmod{m}$

It is noteworthy to mention some properties:

Observation 2.4.1. If $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, then $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$ and $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

Observation 2.4.2. If $ac \equiv bc \pmod{m}$, it need not be true that $a \equiv b \pmod{m}$. If, however, $gcd(c, m) = 1$, it is always true.

Now I should introduce a technique which we will (hopefully) love.
A **Climb Every Mountain Technique** is, when solving a congruence modulo m, we try each value $0, 1, \ldots m-1$. I would say this technique, in Korean, as No-ga-da. This technique is often useful and is only the technique you can use. For example, to solve x such that $x^2 \equiv 3 \pmod{10}$, we substitute $0 \ldots 9$ to x and find out there is no solution.

Theorem 2.4.1 (Linear Congruence Theorem)**.** *Let $a, c, m \in \mathbb{Z}$ with $m \geq 1$ and let $g = gcd(a, m)$.*
(1) If $g \nmid c$, then $\nexists x$ s.t. $ax \equiv c \pmod{m}$.
(2) If $g \mid c$, then $ax \equiv c \pmod{m}$ has exactly g in congruent solutions.

Proof. Proof for (1).
Suppose $\exists x_0$ such that $ax_0 \equiv c \pmod{m}$ when $g \nmid c$.
Then $\exists y$ such that $ax_0 + my = c$.
Now observe that $g \mid a$ thus $g \mid ax_0$ and $g \mid m$ thus $g \mid my$.
Then $g \mid c$ should satisfy, and this is a contradiction.
I omit the proof for (2). □

Arguably, the most important case of **Linear Congruence Theorem** is when $gcd(a, m) = 1$: $ax \equiv c \pmod{m}$. In this case, it has only one solution and denote it as $x \equiv a^{-1}c \pmod{m}$.

I lastly mention **Polynomial Roots Mod p Theorem** and finish this section.

Theorem 2.4.2. *(Polynomial Roots Mod p Theorem)*
Let p be a prime number and let $f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d$ be a polynomial of degree $d \geq 1$ with integer coefficients and with $p \nmid a_0$. Then $f(x) \equiv 0 \pmod{p}$ has at most d incongruent solutions.

I omit the proof.

2.5 Fermat's Little Theorem

Lemma 2.5.1. *Let $a \not\equiv 0 \pmod{p}$. $\{a, 2a, \cdots (p-1)a \pmod{p}\} = \{1, 2, \cdots (p-1) \pmod{p}\}$*

Proof. Note that for $1 \geq k \geq p-1$, $ka \not\equiv 0 \pmod{p}$.
Thus, it is sufficient to show that for $1 \geq i < j \geq p-1$, $ia \not\equiv ja \pmod{p}$.
By the assumptions, $j - i \not\equiv 0 \pmod{p}$ and $a \not\equiv 0 \pmod{p}$, so $(j-i)a \not\equiv 0 \pmod{p}$.
Thus $i \neq j$ and $ia \not\equiv ja \pmod{p}$ is a bijection. □

Theorem 2.5.2 (Fermat's Little Theorem)**.** *Let p be a prime number and a be any number with $a \not\equiv 0 \pmod{p}$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. $a \times 2a \ldots (p-1)a = (p-1)! a^{p-1}$.
By Lemma, $(p-1)! a^{p-1} \equiv (p-1)! \pmod{p}$.
Hence, $a^{p-1} \equiv 1 \pmod{p}$. □

Suppose that we want to calculate $11^{104} \pmod{17}$. We know, by **Fermat's Last Theorem**, that $11^{16} \equiv 1 \pmod{17}$. Thus $11^{96} \equiv 1 \pmod{17}$ and $11^{104} \equiv 11^8 \pmod{17}$. We can then exploit the fact that $11^8 = (11^2)^4$. Since $11^2 \equiv 2 \pmod{17}$, we know that $11^8 \equiv 16 \equiv -1 \pmod{17}$.

Theorem 2.5.3 (Wilson's Theorem)**.** *For a prime number p, $(p-1)! \equiv -1 \pmod{p}$.*

Proof. We first look for trivial cases: when $p = 2, 3$. The theorem holds.
For $p > 3$, it is sufficient to show that $2 \times \ldots (p-2) \equiv 1 \,(\mathrm{mod} p)$.
To show, we look the features of $ax \equiv 1 \,(\mathrm{mod} p)$.
As $gcd(a, p) = 1$, there always exists a unique x; say this a'. If $a = a'$, then $a' \equiv 1 \,(\mathrm{mod} p)$ or $a' \equiv -1 \,(\mathrm{mod} p)$ as

$$\begin{aligned} aa' &\equiv 1 \,(\mathrm{mod} p) \\ a^2 &\equiv 1 \,(\mathrm{mod} p) \\ (a-1)(a+1) &\equiv 0 \,(\mathrm{mod} p) \end{aligned}$$

If $a \neq a'$, then we can always find a pair (a, a') that satisfies $aa' \equiv 1 \,(\mathrm{mod} p)$ by the guaranteed existence and uniqueness of a'.

By the case of $a \neq a'$ above, we notice $(p-2)! \equiv 1 \,(\mathrm{mod} p)$. □

Definition 2.5.1 (Carmichael Number)**.** A composite number m is called a Carmichael number if the congruence $a^{m-1} \equiv 1 \pmod{m}$ is true for every number a with $gcd(a, m) = 1$.

For example, $m = 561 = 3 \cdot 11 \cdot 17$ is a Carmichael number. By Fermat's Little Theorem, we know that $\forall a,\ gcd(a, m) = 1,\ a^2 \equiv 1 \pmod{3},\ a^{10} \equiv 1 \pmod{11},\ a^{16} \equiv 1 \pmod{17}$. Thus, $a^{80} \equiv a^{560} \equiv 1 \pmod{561}$.

2.6 Euler's Formula

The shortcoming of **Fermat's Little Theorem** is that it only works for prime number. However, we are also interested in ks when given some composite number m and a number a that satisfies $a^k \equiv 1 \,(\mathrm{mod} m)$. From the previous knowledge, such is only possible when $gcd(a, m) = 1$. Thus, it is natural to look at the set of numbers that are relatively prime to m.

Definition 2.6.1 (Euler's Phi Function)**.** $\phi(m) = |\{a : 1 \geq a \geq m,\ gcd(a, m) = 1\}|$.

One important feature of Euler's phi function is that, for a given prime number p, $\phi(p) = p - 1$ as every integer $1 \geq a < p$ is relatively prime to p. Also, $\phi(p^k) = p^k - p^{k-1}$.

Theorem 2.6.1 (Euler's Formula)**.** *If $gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \,(\mathrm{mod} m)$.*

Proof. The logic behind the proof is similar to that of **Fermat's Little Theorem**. □

Theorem 2.6.2. *If $gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*

Proof. Define $A = \{a : 1 \leq a \leq mn,\ gcd(a, mn) = 1\}$
$B = \{(b, c) : 1 \leq b \leq m,\ 1 \leq c \leq n,\ gcd(b, m) = gcd(c, n) = 1\}$.
Note that $|A| = \phi(mn)$, $|B| = \phi(m)\phi(n)$.
Now, let $f : A \to B$. It is sufficient to show that f is bijective. In fact, this is implied by **Chinese Remainder Theorem**. □

Theorem 2.6.3 (Chinese Remainder Theorem)**.** *Let m, n be integers such that $gcd(m, n) = 1$. Let b $(0 \leq b \leq m)$ and c $(0 \leq c \leq n-1)$ be any integers. Then $x \equiv b \,(\mathrm{mod} m)$ and $x \equiv c \,(\mathrm{mod} n)$ have exactly one solution where $0 \leq x < mn$.*

I omit the proof for **Chinese Remainder Theorem**. Instead, I give an example written on Sunzi Suanjing:
We have a number of things, but we do not know exactly how many. If we count them by threes, we have the two left over. If we count them by fives, we have three left over. If we count them by sevens, we have two left over. How many things are there?
We are given that $x \equiv 2 \,(\mathrm{mod} 3)$, $x \equiv 3 \,(\mathrm{mod} 5)$, $x \equiv 2 \,(\mathrm{mod} 7)$.
As $3, 5, 7$ are pairwise relatively prime, the given system of congruences have exactly one solution for modulus 105 by **Chinese Remainder Theorem**.
We set $x \equiv 35a_1 + 21a_2 + 15a_3 \,(\mathrm{mod} 105)$. Now our goal is to find a_1, a_2, a_3 such that $35a_1 \equiv$

$2 \pmod 3$, $21a_2 \equiv 3 \pmod 5$, $15a_3 \equiv 2 \pmod 7$.
I first find a_1:

$$\begin{aligned} 35a_1 &\equiv 2 \pmod 3 \\ 35 \cdot 2 \cdot a_1' &\equiv 2 \pmod 3 \end{aligned}$$

Now my goal is to find a_1' such that $35a_1' \equiv 1 \pmod 3$.
As $a_1' \equiv 35^{-1} \pmod 3$, $a_1' = 1$ thus $a_1 = 2$.
By the similar logic, $a_2 = 1$, $a_3 = 1$.
Thus, $x \equiv 23 \pmod{105}$.

Lastly, we look at the relationship between Euler's phi function and sum of divisors.

Observation 2.6.1. Suppose $n = p$ where p is prime. Since $\phi(1) = 1$ and $\phi(p) = p - 1$, $\phi(1) + \phi(p) = p$.

Observation 2.6.2. Suppose $n = p^k$ where p is prime, k some natural number. Then $\phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^k) = p^k$.

Observation 2.6.3. Suppose $n = pq$ where p, q are distinct primes. Then $\phi(1) + \phi(p) + \phi(q) + \phi(pq) = (1 + \phi(p))(1 + \phi(q)) = pq$.

By using these properties, we can come up to **Euler's Phi Function Summation Formula** after a simple lemma.

Lemma 2.6.4. *$\forall n \in \mathbb{N}$, define $F(n) = \phi(d_1) + \phi(d_2) + \cdots + \phi(d_r)$ where ds are the divisors of n. If $gcd(m, n) = 1$ then $F(mn) = F(m)F(n)$.*

Proof. Let $d_1, \ldots d_r$ be the divisors of n, $e_1, \ldots e_s$ be the divisors of m.
Since $gcd(m, n) = 1$, $gcd(d_i, e_j) = 1$ so $\phi(d_i, e_j) = \phi(d_i)\phi(e_j)$.
Hence,

$$\begin{aligned} F(mn) &= \sum_{i,j} \phi(d_i e_j) \\ &= (\phi(d_1) + \phi(d_2) + \cdots + \phi(d_r))(\phi(e_1) + \phi(e_2) + \cdots \phi(e_s)) \\ &= F(m)F(n). \end{aligned}$$

□

Theorem 2.6.5. *(Euler's Phi Function Summation Formula)*
Let $d_1, d_2, \ldots, d_r$ be the divisors of n including 1 and n. Then $\phi(d_1) + \phi(d_2) + \cdots + \phi(d_r) = n$.

Proof. Let $F(n) = \phi(d_1) + \phi(d_2) + \cdots + \phi(d_r)$.
We know by **Observation 2.6.2** that $F(p^k) = p^k$.
Say $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Then

$$\begin{aligned} F(n) = F(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) &= F(p_1^{k_1})F(p_2^{k_2}) \cdots F(p_r^{k_r}) \\ &= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \\ &= n. \end{aligned}$$

□

2.7 Infinite Primes

I start by introducing **Prime Divisibility Theorem** and the **Fundamental Theorem of Arithmetic**.

Theorem 2.7.1 (Prime Divisibility Theorem)**.** *Suppose that for some prime p, if $p \mid a_1 a_2 \cdots a_r$ where $a_1 a_2 \cdots a_r \in \mathbb{Z}_{\geq 2}$, $r \in \mathbb{Z}_{\geq 2}$, then $1 \leq \exists i \leq r$, $p \mid a_i$.*

I omit the proof.

Theorem 2.7.2 (The Fundamental Theorem of Arithmetic)**.** *All natural numbers larger than 1 can be factored into the product of primes in exactly one way.*

Proof. I first prove the existence of the factorisation. I prove by induction.
We check the base case: the theorem holds in case of 2.
We check the inductive case: assume that for $2 \leq \forall n \leq k$, $\forall k \in \mathbb{Z}_{\geq 2}$ the theorem holds.
If $n = k + 1$ is prime, the theorem holds.
If $n = k + 1$ is composite, then we can factorise as $n = n_1 n_2$ where $2 \leq n_1, n_2 \leq k$.
By assumption, n_1, n_2 can be facotored into the product of primes, so n can.

Now I prove the uniqueness of factorisation.
Suppose there are more than one way of factorisation: $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$.
Without loss of generality, say that $p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_s$ does not have common factor.
If they have some, simply erase them and acquire the same form.
Now look p_1. Since $p_1 \mid p_1 p_2 \cdots p_r = n$, $p_1 \mid q_1 q_2 \cdots q_s$.
Then, by **Prime Divisibility Theorem**, $1 \leq \exists i \leq s$, $p_1 \mid q_i$. Contradiction. □

Theorem 2.7.3. *There are infinitely many primes.*

Proof. Suppose there are finite number of primes.
Name each as $p_1, p_2, \ldots p_n$ where n is the number of primes.
Now we inspect the number $x = p_1 p_2 \cdots p_n + 1$.
We observe that x is a composite number as it is not one of the primes we pre-defined.
Since x is a composite number, according to **Fundamental Theorem of Arithmetic**, there must exist some prime number p such that $p \mid x$.
However, we observe there is no such prime number in our predefined prime numbers that can factorise x. This is a contradiction as, according to **Fundamental Theorem of Arithmetic**, all number should be factorised into the product of prime numbers. x is a composite number, so there must exist some prime that can factorise x. □

I provide an example regarding **Theorem 2.7.3** and generalise later to **Dirichlet's Theorem on Primes in Arithmetic Progressions**.

Exercise 2.7.1. Show that there are infinitely many primes that are congruent to 5 (mod 6).

Solution. Suppose that $ps = \{5, p_1, p_2 \ldots p_n\}$ be the finite primes which are congruent to 5 mod 6.
We inspect the number $x = 6p_1 p_2 \cdots p_n + 5$.
First observe that $x \equiv 5 \pmod 6$. Since x is not in pre-defined set ps, x is composite.
Then, by **Fundamental Theorem of Arithmetic**, we can factorise x into product of primes: $x = q_1 q_2 \cdots q_r$ where all qs are primes.
Now, observe that $3 \nmid x$. Thus, $x = 6k + 1$ or $x = 6k + 5$.
Now we look at the features of qs.
If $\forall i$ $q_i \equiv 1 \pmod 6$, then $x = q_1 \cdots q_r \equiv 1 \pmod 6$. We can thus know that at least one q is $\equiv 5 \pmod 6$. Say such q as q'.
Then $q' \in ps$ as ps contain all the primes that is $\equiv 5 \pmod 6$.
If $q' = 5$, then $5 \mid x$. Contradiction.
If $q' = p_t$, $1 \leq t \leq n$, then $q' \mid 6p_1 p_2 \cdots p_r$ and $q' \mid x$.
So $q' \mid 5$, which is a contradiction.

Theorem 2.7.4 (Dirichlet's Theorem on Primes in Arithmetic Progressions)**.** *Let $a, m \in \mathbb{Z}$, $gcd(a, b) = 1$. Then there are infinitely many primes that are congruent to $a \pmod m$.*

I omit the proof.

Finally, I mention **Prime Number Theorem** and move on to next section.

Theorem 2.7.5 (The Prime Number Theorem)**.** *When $x \in \mathbb{Z}$ is large, the number of primes less than x is approximately equal to $\dfrac{x}{lnx}$*

2.8 kth Powers Modulo m and kth Roots Modulo m

Our goal is to compute kth powers modulo m when k and m are very large.

Algorithm 2.8.1. (Successive Squaring to Compute $a^k \pmod m$)

1. Write k as a sum of powers of 2, $k = u_0 + u_1 \cdot 2 + u_2 \cdot 2^2 + \cdots$, where each u_i is either 0 or 1. (binary expansion of k.)

2. Make a table of powers of a modulo m using successive squaring.
   $a^1 \equiv A_0 \pmod m$
   $a^2 \equiv A_0^2 \equiv A_1 \pmod m$
   $\vdots$
   $a^{2^r} \equiv A_{r-1}^2 \equiv A_r \pmod m$

3. The product $A_0^{u_0} \cdot A_1^{u_1} \cdots A_r^{u_r} \pmod m$ will be congruent to $a^k \pmod m$.

As an example, I compute $2^{9990} \pmod{9991}$.
First, I convert 9990 to binary: $9990 = 2^{13} + 2^{10} + 2^9 + 2^8 + 2^2 + 2^1$.
Then, I look at the able of powers of 2 modulo m: Finally,

2^1	2^2	2^4	2^8	2^{16}	2^{32}	2^{64}
2	4	16	256	5590	6243	158
2^{128}	2^{256}	2^{512}	2^{1024}	2^{2048}	2^{4096}	2^{8192}
4982	2680	8862	5784	4788	5590	6243

Table 2.1: Table of Powers of 2 modulo m

$$\begin{aligned} 2^{9990} &\equiv 6243 \cdot 5784 \cdot 8862 \cdot 2680 \cdot 16 \cdot 4 \pmod{9991} \\ &\equiv 2038 \cdot 8862 \cdot 2680 \cdot 16 \cdot 4 \pmod{9991} \\ &\equiv 7019 \cdot 2680 \cdot 16 \cdot 4 \pmod{9991} \\ &\equiv 7858 \cdot 64 \pmod{9991} \\ &\equiv 3362 \pmod{9991} \end{aligned}$$

Now, we try to compute kth roots modulo m. In other words, suppose we are given b and told to find x such that $x^k \equiv b \pmod m$. We limit as $gcd(b, m) = 1$ and $gcd(k, \phi(m)) = 1$.

Algorithm 2.8.2. (Compute kth Roots Modulo m)

1. Compute $\phi(m)$.

2. Find positive integers u and v such that $ku - \phi(m)v = 1$. In other words, find a positive integer u such that $ku \equiv 1 \pmod{\phi(m)}$.

3. Compute $b^u \pmod m$ by successive squaring.

$gcd(k, \phi(m)) = 1$ is necessary as we can only find solutions u and v for $ku - \phi(m)v = 1$ under such limit. For better understanding, I provide an example: find x which satisfies $x^k \equiv b \pmod m$.
First, compute $\phi(1073)$: $\phi(1073) = \phi(29)\phi(37) = 1008$.
Next, I find positive integer solutions to the equation $131u - 1008v = 1$ by Linear Equation Theorem. I first apply Euclidean algorithm and check that $gcd(131, 1008) = 1$:

$$\begin{aligned} 1008 &= 131 \cdot 7 + 91 \\ 131 &= 91 \cdot 1 + 40 \\ 91 &= 40 \cdot 2 + 11 \\ 40 &= 11 \cdot 3 + 7 \\ 11 &= 7 \cdot 1 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \end{aligned}$$

Now we back-trace and find u, v:

$$\begin{aligned}
1 &= 4 - 3 = 4 - (7 - 4) \\
&= 4 \cdot 2 - 7 = (11 - 7) \cdot 2 - 7 \\
&= 11 \cdot 2 - 7 \cdot 3 = 11 \cdot 2 - (40 - 11 \cdot 3) \cdot 3 \\
&= 11 \cdot 11 - 40 \cdot 3 = (91 - 40 \cdot 2) \cdot 11 - 40 \cdot 3 \\
&= 91 \cdot 11 - 40 \cdot 25 = 91 \cdot 11 - (131 - 91) \cdot 25 \\
&= 91 \cdot 36 - 131 \cdot 25 = (1008 - 131 \cdot 7) \cdot 36 - 131 \cdot 25 \\
&= 1008 \cdot 36 - 131 \cdot 277
\end{aligned}$$

By Linear Equation Theorem, the solution is expressible as $(u, v) = (-277 - 1008k, -36 - 131k)$.
We thus can find positive integer solution $(731, 95)$.
Now I explain why we compute $758^{731} \pmod{1073}$, third step of **Algorithm 2.8.2**.
We observe that $(x^{131})^{731} = x^{131 \cdot 731} = x^{1+1008 \cdot 95} = x \cdot (x^{1008})^{95}$.
As $\phi(1073) = 1008$, we know that $x^{1008} \equiv 1 \pmod{1073}$; hence, $x \equiv (x^{131})^{731} \equiv 758^{731} \pmod{1073}$.
Now we use successive squaring and compute $758^{731} \pmod{1073}$. Doing so, we acquire $x \equiv 905 \pmod{1073}$.

2.9 Squares Modulo p

So far, we only looked at $ax \equiv c \pmod{m}$. This chapter focuses on $x^2 \equiv c \pmod{m}$.

Definition 2.9.1. (Quadratic Residue Modulo p (QR) and NR)
A nonzero number that is congruent to a square modulo p is called a quadratic residue modulo p. A number that is not congruent to a square modulo p is called a (quadratic) nonresidue modulo p. QR and NR are abbreviations, respectively.

For example, the full set of QRs modulo 7 is $\{1, 2, 4\}$ and the full set of NRs modulo 7 is $\{3, 5, 6\}$, as can be seen by the table.

x	0	1	2	3	4	5	6
c	0	1	4	2	2	4	1

Table 2.2: Table of squares modulo 7

Theorem 2.9.1. *Let p be an odd prime. There are exactly $\frac{p-1}{2}$ QRs and NRs.*

Proof. It is enough to show that $1^2, 2^2, \ldots (\frac{p-1}{2})^2 \pmod{p}$ are all different.
To prove, assume $\exists 1 \leq b_1 \neq b_2 \leq \frac{p-1}{2}$ such that $b_1^2 \equiv b_2^2 \pmod{p}$.
Then $p \mid b_1^2 - b_2^2 = (b_1 + b_2)(b_1 - b_2)$.
Note that $2 \leq b_1 + b_2 \leq p - 1$, so $p \mid b_1 - b_2$. This is a contradiction as there is no such $b_1 \equiv b_2 \pmod{p}$.

Definition 2.9.2. (Legendre Symbol of a modulo p)
The Legendre symbol of a modulo p is $\left(\frac{a}{p}\right) = 1$ if a is a quadratic residue modulo p, and $\left(\frac{a}{p}\right) = -1$ if a is a quadratic nonresidue modulo p.

Theorem 2.9.2. *(Quadratic Residue Multiplication Rule)*
Let p be an odd prime. Then:

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

□

The theorem implies that $QR \times QR = QR$, $QR \times NR = NR$, $NR \times NR = QR$.

Exercise 2.9.1. Compute $\left(\frac{75}{97}\right)$

Solution. Our goal is to find x such that $x^2 \equiv 75 \pmod{97}$.
By Quadratic Residue Multiplication Rule, $\left(\frac{75}{97}\right) = \left(\frac{5^2}{97}\right)\left(\frac{3}{97}\right) = \left(\frac{3}{97}\right)$.
We observe that $10^3 \equiv 3 \pmod{97}$, thus $\left(\frac{3}{97}\right) = 1$. Hence, $\left(\frac{75}{97}\right) = 1$.

2.10 Study on -1 and 2 Square Modulo p

We start by thinking which primes p is $\left(\frac{-1}{p}\right) = 1$.

p	3	5	7	11	13	17	19	23	29	31
Sol	NR	2, 3	NR	NR	5, 8	4, 13	NR	NR	12, 17	NR

Table 2.3: Table of solutions to $x^2 \equiv 1 \pmod{p}$

It seems like if $p \equiv 1 \pmod 4$ then -1 is QR, and if $p \equiv 3 \pmod 4$ then -1 is NR. In fact, it is. To verify such tendency, we look for *Square Root of Fermat's Little Theorem.*

Let $A = a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$, $a \not\equiv 0 \pmod{p}$.
Then by $A^2 \equiv 1 \pmod{p}$ by Fermat's Little Theorem. This means that $p \mid A^2 - 1 = (A-1)(A+1)$. Hence, $p \mid A-1$ or $p \mid A+1$, which means $A \equiv 1 \pmod{p}$ or $A \equiv -1 \pmod{p}$.

Theorem 2.10.1. *(Euler's Criterion)*
Let p be an odd prime. Then

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

Proof. Suppose that a is QR, say $a \equiv b^2 \pmod{p}$. Then, by Fermat's Little Theorem,

$$a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} = b^{p-1} \equiv 1 \pmod{p}.$$

Hence $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.
We then should prove that all solutions to $x^{(p-1)/2} \equiv 1 \pmod{p}$ are exactly same to the set of QRs.
We just proved that every QR is a solution to the congruence above, and there are exactly $\frac{p-1}{2}$ distinct QRs. Also, by Polyomial Roots Mod p Theorem, it has at most $\frac{p-1}{2}$ distinct solutions. Hence,

$$\{\text{solutions to } x^{(p-1)/2} - 1 \equiv 0 \pmod{p}\} = \{\text{quadratic residues modulo p}\}.$$

Now suppose that a is NR. We know that $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem. Thus

$$0 \equiv a^{p-1} - 1 \equiv (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \pmod{p}.$$

We know that $a^{(p-1)/2} - 1 \not\equiv 0 \pmod{p}$ as we previously showed the solutions to $x^{(p-1)/2} - 1 \equiv 0 \pmod{p}$ are the QRs. Hence,

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

□

Euler's Criterion clearly shows the tendency is true. As $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2}$, if $p \equiv 1 \pmod 4$ then $(-1)^{(p-1)/2} = 1 = \left(\frac{-1}{p}\right)$; if $p \equiv 3 \pmod 4$ then $(-1)^{(p-1)/2} = -1 = \left(\frac{-1}{p}\right)$.

There is another interesting feature when inspecting the case of 2 instead of -1. As we did previously, we look for primes p such that $\left(\frac{2}{p}\right) = 1$.

p	3	5	7	11	13	17	19	23	29	31
$x^2 \equiv 2$	NR	NR	3, 4	NR	NR	6, 11	NR	5, 18	NR	8, 23
$p \pmod 8$	3	5	7	3	5	1	3	7	5	7
p	37	41	43	47	53	59	61	67	71	73
$x^2 \equiv 2$	NR	17, 24	NR	7, 40	NR	NR	NR	NR	12, 59	32, 41
$p \pmod 8$	5	1	3	7	5	3	5	3	7	1

Table 2.4: Table of solutions to $x^2 \equiv 2 \pmod p$ and $p \pmod 8$

We observe the tendency that $\left(\frac{2}{p}\right) = 1$ or -1, if $p \equiv 1, 7 \pmod 8$ or $p \equiv 3, 5 \pmod 8$, respectively. Unfortunately, we cannot use Euler's Criterion as calculating $2^{(p-1)/2} \pmod p$ is not easy. However, Gauss came up with a brilliant idea:
Say that we want to check if 2 is a quadratic residue modulo 17. Then we find that

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \cdot 14 \cdot 16 &= (2 \cdot 1)(2 \cdot 2)(2 \cdot 3)(2 \cdot 4)(2 \cdot 5)(2 \cdot 6)(2 \cdot 7)(2 \cdot 8) \\ &= 2^8 \cdot 8!. \end{aligned}$$

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \cdot 14 \cdot 16 &\equiv 2 \cdot 4 \cdot 6 \cdot 8 \cdot (-7) \cdot (-5) \cdot (-3) \cdot (-1) \\ &\equiv (-1)^8 \cdot 8! \pmod{17} \end{aligned}$$

so $2^8 \equiv 1 \pmod{17}$, thus 2 is a quadratic residue modulo 17.
Generalising this idea, we can reach

$$2^{(p-1)/2} \equiv (-1)^{(\text{number of integers in } \{2,4,6,\ldots,p-1\} \text{larger than (p - 1) / 2.})} \pmod p$$

Using this idea, it is not difficult to verify the tendency of $\left(\frac{2}{p}\right)$.

2.11 Quadratic Reciprocity

Theorem 2.11.1. *(Law of Quadratic Reciprocity)*
Let p and q be distinct odd primes.

1. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \end{cases}$
2. $\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 7 \pmod 8 \\ -1, & \text{if } p \equiv 3, 5 \pmod 8 \end{cases}$
3. $\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right), & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right), & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4 \end{cases}$

The third one can be rewritten as: $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.
Let me use the following features without proof:

1. I introduce a Jacobi symbol, which is a generalised version of Legendre symbol. For any integer a and positive odd integer b factored into product of primes $b = p_1 p_2 \cdots p_r$, then $\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)$.
2. We can use the Law of Quadratic Reciprocity when a and b are odd positive integers. This is called *Generalised Law of Quadratic Reciprocity.*

2.12 Primitive Roots and Indices

For $gcd(a, p) = 1$, Fermat's Little Theorem tells us that $a^{p-1} \equiv 1 \pmod{p}$; however, this does not mean that $p - 1$ is the smallest exponent e that makes $a^e \equiv 1 \pmod{p}$. For example, $2^3 \equiv 1 \pmod{7}$.

$p = 7$
$1^1 \equiv 1 \pmod{7}$
$2^3 \equiv 1 \pmod{7}$
$3^6 \equiv 1 \pmod{7}$
$4^3 \equiv 1 \pmod{7}$
$5^6 \equiv 1 \pmod{7}$
$6^2 \equiv 1 \pmod{7}$

Table 2.5: Table of Smallest Power of a that equals 1 Modulo 7

From the table, we can make two observations.

Observation 2.12.1. The smallest exponent e such that $a^e \equiv 1 \pmod{p}$ seems to divide $p - 1$.

Observation 2.12.2. There are always some a's that require the exponent $p - 1$.

Before moving on, I define what is called the *order of a modulo p.*

Definition 2.12.1. (Order of a modulo p)
$e_p(a)$ is the smallest exponent $e \geq 1$ such that $a^e \equiv 1 \pmod{p}$.

Let me move on without proving the observations. What we should focus on instead is the numbers that require the largest possible order: $e_p(a) = p - 1$. If a is such a number, then the powers $a, a^2, \ldots, a^{p-1} \pmod{p}$ must have all different modulo p. Here, we have another important definition.

Definition 2.12.2. (Primitive Root Modulo p)
A number g with maximum order $e_p(g) = p - 1$ is called a primitive root modulo p.

Theorem 2.12.1. *(Primtive Root Theorem)*
There are exactly $\phi(p - 1)$ primitive roots modulo p.

The beauty of a primitive root g modulo a prime p is the appearance of every nonzero number modulo p as a power of g. So for any number $1 \leq a < p$, we can pick out exactly one of the powers $g, g^2, \ldots, g^{p-1}$ as being congruent to a modulo p. The exponent is called the *index of a modulo p for the base g.* We write $I(a)$ for the index.

a	1	2	3	4	5	6	7	8	9	10	11	12
$I(a)$	12	1	4	2	9	5	11	3	8	10	7	6

Table 2.6: Table of Indices Modulo 13 for Base 2

Theorem 2.12.2. *(Rules for Indices)*
Indices satisfy the following rules:

1. $I(ab) \equiv I(a)I(b) \pmod{p-1}$
2. $I(a^k) \equiv kI(a) \pmod{p-1}$

This makes our life easier. For example, suppose we want to get the solution of $19x \equiv 23 \pmod{37}$. We can use the following trick:

$$\begin{aligned} 7x &\equiv 12 \pmod{13} \\ I(7x) &\equiv I(12) \pmod{13} \\ I(7) + I(x) &\equiv I(12) \pmod{13} \\ 11 + I(x) &\equiv 6 \pmod{13} \\ I(x) &\equiv -5 \equiv 8 \pmod{13}. \end{aligned}$$

We check the table of indices modulo 13 for base 2 and get that $x \equiv 9 \pmod{13}$.

Chapter 3

Topology

3.1 Set Theory

To do...

Bibliography

[Tem02] Temporary. Discovery of Pleiades Cluster Network (DPCN). *Temporary*, 99(9):99–999, 2002.