Individual

Number Theory, Topology, Real and Complex Analysis

Individual Project during 2023 Summer

Note

Author:
Hyunjun Choi

June 29, 2023

Contents

List of Figures

List of Tables

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 $c + b = s^2$, $c - b = t^2$.

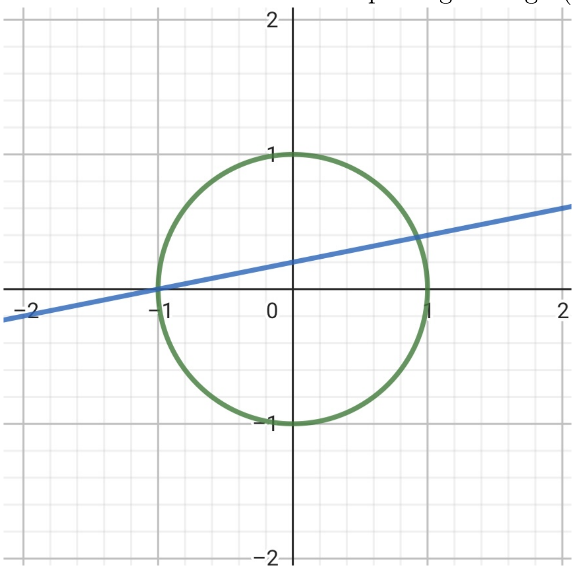
It is worth noting the relationship between the PPT and unit circle. We start by dividing the both sides of $a^2 + b^2 = c^2$ by c^2. Then we can induce the typical unit circle form by substituting as $x = \dfrac{a}{c}$ and $y = \dfrac{b}{c}$. Our goal is to find (x, y) where $x, y \in \mathbb{Q}$.

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, it is worth noting that $gcd(a, b) \times lcm(a, b) = ab$.

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 $0, 1, \dots m - 1$. 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 $0 \dots 9$ 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 $x \equiv a^{-1}c \pmod{m}$.

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. $a \times 2a \dots (p-1)a = (p-1)!a^{p-1}$.
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 $2 \times \dots (p-2) \equiv 1 \pmod{p}$.
To show, we look the features of $ax \equiv 1 \pmod{p}$.
As $gcd(a, p) = 1$, there always exists a unique x; say this a'. If $a = a'$, then $a' \equiv 1 \pmod{p}$ or $a' \equiv -1 \pmod{p}$ as

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

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

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

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 $a^k \equiv 1 \pmod{m}$. 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 $a^{\phi(m)} \equiv 1 \pmod{m}$.*

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 $x \equiv b \pmod{m}$ and $x \equiv c \pmod{n}$ 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 $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$.
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 $x \equiv 35a_1 + 21a_2 + 15a_3 \pmod{105}$. 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:

$$35a_1 \equiv 2 \pmod{3}$$
$$35 \cdot 2 \cdot a_1' \equiv 2 \pmod{3}$$

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, $x \equiv 23 \pmod{105}$.

Chapter 3

Topology

3.1 Set Theory

To do...

Bibliography

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