XM452 Lecture Notes 1

Erdaifu Luo

19 February 2023

§1 Introduction to Number Theory

§1.1 Notation

The integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$.
The rational numbers $\mathbb{Q}\{m/n : m, n \in \mathbb{Z}\}$.
The real number $\mathbb{R}$.
Those $x \in \mathbb{R}$ such that$x \notin \mathbb{Q}$, are called irrational.

§1.2 Primes and Composites

Definition 1.1 (Prime Numbers)**.** An integer greater than one whose only positive (integer) divisors are itself and one is called a **prime number**.

Definition 1.2 (Composite Number)**.** An integer greater than one which is not a prime number is said to be **composite**. So if $n \in \mathbb{Z}$ is a composite number then

$$n = ab, \text{where } a, b \in \mathbb{Z}, a, b > 1.$$

If a is composite, we can write

$$a = a_1 \cdot a_2,$$

where

$$a_1, a_2 \in \mathbb{Z}, a_i > 1.$$

Proposition 1.3

If n is a composite integer, then n can be written as a product of primes

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k.$$

where the p_i's are prime.

This decomposition is unique except for the order of the p_i's.

Definition 1.4 (Divides)**.** When an integer a divides into an integer b so that the quotient $b/a \in \mathbb{Z}$, we write $a \mid b$ and say that "a divides b".

Theorem 1.5

There are infinite many primes.

Proof. Assume the contrary. That is there are finitely many primes. We'll write them in a list: $p_i \dots p_k$.

Let $N = p_i \dots p_k + 1$. Notice that $N > p_i \mid N$ for each i so N is not a prime. Therefore, N is a composite integer. By the above proposition, there exists a prime that divides into N.

Since every prime is in the list $p_i \dots p_k$, then for some i, $p_i \mid N$. That is,

$$p_i \mid p_i \dots p_k + 1.$$

On the other hand, clearly

$$p_i \mid p_i \dots p_k,$$

which means that $p_i \mid N - 1$. So we have

$$p_i \mid N - 1 \text{ and } p_i \mid N.$$

Say $p_i \cdot u = N - 1$ and $p_i \cdot v = N$, where $u, v \in \mathbb{Z}$ and $u, v > 0$. Subtracting,

$$p_i \cdot v - p_i \cdot u = N - (N - 1) = 1,$$

meaning that $p_1 \cdot (v - u) = 1$.

That statement was a contradiction (you cannot have the product of two integers where one is a prime equal 1), which means that the original statement is false, and there exist infinite primes. □

§2 Famous Theorems about Primes

Theorem 2.1

n is prime if, and only if, $n \mid ((n-1)! + 1)$.

§3 Pythagorean Triples, Diophantine Equations, Fermat's Last Theorem

§3.1 Proof of Pythagorean Triples

Determining whether an integer is prime or composite, or questions related to such are examples of **multiplicative questions** in number theory.

Another category of questions are **additive questions**.

Example 3.1

When is a perfect square integer the sum of two perfect squares (e.g. $5^2 = 3^2 + 4^2$)?

Proof. Due to the Pythagorean theorem, this question is equivilant to the sum of two perfect square integers, which is equivilant to the magnitude of c when there is a right triangle a, b and c with $a, b, c \in \mathbb{Z}$.

By observing Pythagorean triples, we can see that some triples are $(3, 4, 5)$ and $(5, 12, 13)$ where $c = b + 1$ where b is an arbitary side.

Therefore, we need to find integers a, b, c such that:

(1) $a^2 + b^2 = c^2$

(2) $b + 1 = c$

Substituting,

$$\begin{aligned} a^2 + b^2 &= (b+1)^2 \\ &= b^2 + 2b + 1 \\ a^2 &= 2b + 1. \end{aligned}$$

So, since odd numbers are represented as $o = 2n + 1$ where $n \in \mathbb{Z}$, so a itself must be an odd number, and $a = 2n + 1$.

So now,

$$a^2 = 2b + 1$$

can be written as

$$\begin{aligned} (2n+1)^2 &= 2b + 1 \\ \frac{(2n+1)^2 - 1}{2} &= b \\ \frac{4n^2 + 4n}{2} &= b \\ 2n^2 + 2n &= b. \end{aligned}$$

But by (2), $b + 1 = c$, therefore

$$2n^2 + 2n + 1 = c.$$

So for any $n \in \mathbb{Z}$ such that $n > 0$,

$$(2n + 1, 2n^2 + 2n, 2n^2 + 2n + c)$$

is an Pythagorean triples. □

§3.2 Diophantine Equations

Equations of the form $x^2 + y^2 = z^2$ are called **Diophantine Equations**.

§3.3 Fermat's Last Theorem

Theorem 3.2 (Fermat's Last Theorem)
If $x \neq 2$, then $x^n + y^n = z^n$ has no solutions where x, y and z are all nonzero integers.

§4 The Euclidean Algorithm

Definition 4.1. Let $a, b \in \mathbb{Z}$. The set of **common divisors** of a and b is the set, $\{m \in \mathbb{Z}$ such that $m \mid a$ and $m \mid b\}$.

If $a = b = 0$, then the set of common divisors is the set of all integers.
If a and b are not both zero, then this set is finite, and always contains 1.
Therefore there is always a largest number in this set.

Definition 4.2. If $a, b \in \mathbb{Z}$ are not both zero, then the largest number in the set of common divisors of a and b is called the **greatest common divisor** (GCD).

if d is this number, we write $d = (a, b)$.

The **Euclidean Algorithm** is a method for finding the GCD. The basic principle is that if $n \mid a$ and $n \mid b$, then for any integer r and s, $n \mid (r \cdot a + s \cdot b)$.

Theorem 4.3 (Euclidean Algorithm)

If a and b are positive integers, $b > a$, and r_k is found using the Euclidean Algorithm method, then

$$r_k = (a, b).$$

Moreover, from these equations there is a systematic way to find integers m and n such that

$$r_k = ma + nb.$$

§5 Proof of the Euclidean Algorithm

Proof. Let $d = (a, b)$. Rewrite the equation in the form

$$\begin{aligned}
r_0 &= a - q_0 \cdot b \\
r_1 &= b - q_1 \cdot r_0 \\
r_2 &= r_0 - q_2 \cdot r_1 \\
&\vdots \\
r_k &= r_{k-2} - q_k \cdot r_{k-1} \\
0 &= r_{k-1} - q_{k+1} \cdot r_k
\end{aligned}$$

□

Since $d \mid a$ and $d \mid b$, $d \mid (a - q_0 \cdot b)$, meaning that $d \mid r_0$. Furthermore, $d \mid (b - q_1 \cdot r_0)$, meaning that $d \mid r_1$.

Similarily, $d \mid r_2$, $d \mid r_3$, $\ldots$,$d \mid r_k$. Thus, $d \leq r_k$.

Since $r_{k-1} = q_{k-1} \cdot r_k$,

$$r_k \mid r_{k-1}.$$

Similarly, since $r_{k-2} = q_k \cdot r_{k-1} + r_k$,

$$r_k \mid r_{k21}.$$

Continuing, $r_k \mid r_{k-3}$, $r_k \mid r_{k-4}$, $\ldots r_k \mid r_1$, $r_k \mid r_0$. But $b = q_1 r_0 + r_1$, so $r_k \mid b$, and $a = q_0 b + r_0$, so $r_k \mid a$.

So r_k is common divisor of a and b with $a \neq b$. Thus, $r_k \leq (a, b) = d \leq r_k$, so $d = r_k$.

$r_k = ma + nb$, with $m, n \in \mathbb{Z}$, is called a **linear combination of a and b**. If we can write r_{j-1} and r_{j-2} as linear combinations of a and b, then we use the equation

$$r_j = r_{j-2} - q_j r_{j-1}$$

to express r_j as a linear combination of a and b.

Let S_j be the statement that there are integers m_{j-2}, n_{j-2}, m_{j-1}, n_{j-1}, such that

$$\begin{aligned}
r_{j-2} &= m_{j-2} a + n_{j-2} b \\
r_{j-1} &= m_{j-1} a + n_{j-1} b
\end{aligned}$$

Claim 5.1 — Statement S_k is true.

Proof. By induction,

Base Case: Let $r_{-2} = a$ and $r_{-1} = b$. Then

$$\begin{aligned} r_{-2} &= a = 1 \cdot a + 0 \cdot b \\ r_{-1} &= b = 0 \cdot a + 1 \cdot b \end{aligned}$$

Thus, S_0 is true with $m_{-2} = 1$, n_{-2}, $m_{-1} = 0$, and $n_{-1} = 1$.

Inductive case: Assume S_j holds, i.e.

$$\begin{aligned} r_{j-2} &= m_{j-2}a + n_{j-2}b \\ r_{j-1} &= m_{j-1}a + n_{j-1}b \end{aligned}$$

Inductive step: Show S_{j+1} holds, i.e.

$$\begin{aligned} r_{j-1} &= m_{j-1}a + n_{j-1}b \\ r_j &= m_j a + n_j b \end{aligned}$$

By S_j,

$$r_{j-1} = m_{j-1}a + n_{j-1} \cdot b.$$

Find m_j and n_j so that $r_j = m_j \cdot a + n_j \cdot b$.

We know

$$\begin{aligned} r_{j-2} &= q_j r_{j-1} + r_j \\ r_j &= r_{j-2} - q_j r_{j-1} \end{aligned}$$

Substituting,

$$\begin{aligned} r_j &= (m_{j-2}a + n_{j-2}b) - q(m_{j-1}a + n_{j-1}b) \\ &= (m_{j-2}a - q_j mj - 1)a - (n_{j-2} - qjnj - 1)b. \end{aligned}$$

Then, $r_j = m_j \cdot a + n_j \cdot b$. $\square$