Number Theory

John is peeking into Numbertheory

Author: John Pink

Date: September 9, 2023

Version: 4.3

Victory won't come to us unless we go to it.

Contents

Chapter 1 Natural Number

What is natural number? Just like what they are called. Long time ago, human counted numbers will like this " one, two, three, ...". So naturally we can define natural numbers like this

Definition 1.1 (Natural Number)

$$\mathbb{N} := \{1, 2, 3, \cdots\}$$

♣

1.1 Primes

Theorem 1.1 (Euclid)

There are infinitely many primes.

♡

Proof If there is only finitely many primes, we can list them as$p_1, p_2, \cdots, p_r$. Let

$$N = p_1 p_2 \cdots p_r + 1.$$

By the Fundamental Theorem of Arithmetic, N can be factorized, so it must be divisible by some prime p_k of our list. Since p_k also divides $p_1 p_2 \cdots p_r$, it must divide their difference

$$p_k | N - p_1 p_2 \cdots p_r = 1$$

which is impossible, as $p_k > 1$. $\square$

Chapter 2 Congruent

2.1 Congruent

Definition 2.1

We assign two integers a and b which have the same remainder mod n to the same residue class mod n or more simply, the same class mod n, and write

$$a \equiv b(\text{mod } n)$$

Theorem 2.1

$$a \equiv b(\mod n) \Longleftrightarrow n|a-b$$

Theorem 2.2

If $ca \equiv cb(\mod n)$, then

$$a \equiv b\left(\mod \frac{n}{d}\right), where (c,n)=d$$

and conversely.

Proposition 2.1 (properties of congruent)

1. $a \equiv a(\mod n)$
2. *If $a \equiv b(\mod n)$, then $b \equiv a(\mod n)$*
3. *If $a \equiv b(\mod n)$ and $b \equiv c(\mod n)$, then $a \equiv c(\mod n)$*
4. *If $a \equiv b(\mod n)$ and $c \equiv d(\mod n)$, then $a \pm c \equiv b \pm d(\mod n)$.*
5. *If $a \equiv b(\mod n)$, then $ac \equiv bc(\mod n)$.*
6. *If $a \equiv b(\mod n)$ and $c \equiv d(\mod n)$, then $ac \equiv bc(\mod n)$.*
7. *If $a \equiv b(\mod n)$, then $f(a) \equiv f(b)(\mod n)$, when $f(x)$ is an integral function of x (polynomial in x) with integral coefficients.*

Corollary 2.1

If $a \equiv b(\mod n)$, then $\forall n \in \mathbb{N}$,

$$a^k \equiv b^k(\mod n)$$

Theorem 2.3

If $x_1, x_2, \ldots, x_n$ forms a complete system of residues mod n ($n > 0$), then $ax_1+b, \ldots, ax_n+b$ is also such a system, as long as a and b are integers and $(a,n)=1$.

Proof To prove the theorem, we just need to prove that

$$ax_i + b \not\equiv ax_j + b(\mod n)\ (i \neq j)$$

Conversely, we let $ax_i + b \equiv ax_j + b(\mod n)$, by property (iv), we have $ax_i \equiv ax_j(\mod n)$, and because $(a,n)=1$. By property (vi), we know $x_i \equiv x_j(\mod n)$. Finally, because $x_1, x_2, \ldots, x_n$ forms a complete system of residues mod n. We finally get $i=j$.

Theorem 2.4

If $a_1, a_2, \ldots, a_n$ are pairwise relatively prime integers, then a complete residue system mod A, where $A = a_1 a_2 \ldots a_n$, is obtained in the form

$$L(x_1, x_2, \ldots, x_n) = \frac{A}{a_1} c_1 x_1 + \frac{A}{a_2} c_2 x_2 + \cdots + \frac{A}{a_n} c_n x_n$$

if the x_i independently run through a complete residue system mod a_i $(i = 1, 2, \ldots, n)$. Here the c_i may be arbitary integers relatively prime to a_i. ♡

Proof The number of these L values is $|A|$, because every x_i runs through a complete residue system mod a_i will produce a_i values. So we just need to prove for every two L when x_i run through a complete residue system mod a_i, they have different congruent mod A.
To do this, we let

$$L(x_1, \ldots, x_n) \equiv L(x'_1, \ldots, x'_n) \pmod{A}$$

A.K.A (as known as)

$$\frac{A}{a_1} c_1 x_1 + \cdots + \frac{A}{a_n} c_n x_n \equiv \frac{A}{a_1} c_1 x'_1 + \cdots + \frac{A}{a_n} c_n x'_n \pmod{A}$$

Since $a_1 | A = a_1 a_2 \cdots a_n$

$$\frac{A}{a_1} c_1 x_1 + \cdots + \frac{A}{a_n} c_n x_n \equiv \frac{A}{a_1} c_1 x'_1 + \cdots + \frac{A}{a_n} c_n x'_n \pmod{a_1}$$

and because $\frac{A}{a_i} c_i x_i \equiv 0 \pmod{a_1}$ $(i \neq 1)$ we get

$$\frac{A}{a_1} c_1 x_1 \equiv \frac{A}{a_1} c_1 x'_1$$

Moreover by theorem2.1, since $(c_1, a_1) = 1$ and $\left(\frac{A}{a_1}, a_1\right) = 1$, we get $x_1 \equiv x'_1 \pmod{a_1}$ Exactly, as the same way above, we can get $x_i \equiv x'_i \pmod{a_i}$ for all i.

Definition 2.2 (Euler Phi function)

$$\varphi(n) := \#\{i (0 \leq i \leq n-1) | (i, n) = 1\}$$

where # means the element number of a set. ♣

Theorem 2.5 (Fermat-Euler Theorem)

$\forall a \in \mathbb{Z}$, if $(a, n) = 1$, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

where $\varphi(n)$ is Euler-phi function. ♡

Proof [Fermat]

1. If $a = 1$, obviously $1^p = 1 \equiv 1 (\mathrm{mod} p)$
2. Assume for some $b \in \mathbb{N}$, $b^p \equiv b (\mathrm{mod} p)$, we just need to prove for $a = b + 1$, we have $a^p \equiv a \pmod{p}$.
   By binomial theorem, we have

$$(b+1)^p = \sum_{i=0}^{p} \left(\begin{array}{c} p \\ i \end{array} \right) b^i, \ where \left(\begin{array}{c} p \\ i \end{array} \right) = \frac{p(p-1)\cdots(p-i+1)}{i!}$$

If $1 \leq i \leq p-1$, then $p \left| \begin{pmatrix} p \\ i \end{pmatrix} \right.$. Since

$$i! \begin{pmatrix} p \\ i \end{pmatrix} = p(p-1)(p-2)\cdots(p-i+1)$$

Naturally, we have

$$p \left| i! \begin{pmatrix} p \\ i \end{pmatrix} \right.$$

Since p is a prime and $1 \leq i < p$, $(p, i!) = 1$, so we have

$$p \left| \begin{pmatrix} p \\ i \end{pmatrix} \right.$$

Finally

$$\begin{aligned} (b+1)^p &= \sum_{i=0}^{p} \begin{pmatrix} p \\ i \end{pmatrix} b^i \\ &= b^p + 1 + \sum_{i=1}^{p-1} \begin{pmatrix} p \\ i \end{pmatrix} b^i \\ &\equiv b^p + 1 (\mod p) \\ &\equiv b + 1 (\mod p) \end{aligned}$$

Theorem 2.6

For given polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, and prime P, meantime $a_n \not\equiv 0(\mod P)$, then

$$f(x) \equiv 0(\mod P)$$

the numbers of root is less than or equal to $\deg f(x) = n$

Remark We mark $\mathbb{Z}/p\mathbb{Z}$ as $\mathbb{F}_p$, which means $\mathbb{Z}/p\mathbb{Z}$ is a **finite field**. And $\mathbb{Z}/p\mathbb{Z}$ presents a complete system of residues mod p.

The above theorem can be equivalently described as below

Theorem 2.7 (Lagrange Theorem)

For given polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{F}_p[x]$, and prime P, meantime $a_n \neq 0,\ in\ \mathbb{F}_p[x]$, then

$$f(x) = 0,\ in\ \mathbb{F}_p[x]$$

the numbers of root is less than or equal to $\deg f(x) = n$

Definition 2.3 (Equal)

Two integral polynomial

$$f(x) = c_0 + c_1 x + \cdots + c_k x^k$$

$$g(x) = a_0 + a_1 x + \cdots + a_l x^l$$

when $k = l$ and $c_i = a_i(\mod n)$ for $i = 0, 1, 2, \ldots, k$, we say $f(x)$ and $g(x)$ are congruent modulo n.

$$f(x) \equiv g(x)(\bmod n)$$

Theorem 2.8

If $(a, n) = 1$, then the congruence equations

$$ax + b \equiv 0(\bmod n)$$

exactly have one root $\mod n$.

Proof By 2.1 $ax + b$, when x runs through a complete residue system mod n, its value exactly is equal to 0 once, so the solution of the equation is unique $\bmod n$.

Theorem 2.9 (Wilson Theorem)

If p is a prime, then

$$(p - 1)! \equiv -1(\bmod p)$$

Theorem 2.10

Suppose $n \in \mathbb{N}$ and $n > 1$, then

$$n \text{ is a prime} \iff (n - 1)! \equiv -1(\bmod n)$$

Definition 2.4 (Carmichael number)

Suppose n is a composite number. If $\forall a \in \mathbb{Z}$ and $(a, n) = 1$, if the below equation is always established

$$a^{n-1} \equiv n(\bmod n)$$

then we call n as a Carmichael number or a absolutely improper number.

Theorem 2.11 (Chinese Remainder Theorem)

Suppose that $n_1, n_2, \ldots, n_k \in \mathbb{N}$ which are pairwise prime, and $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. Let $v = n_1, n_2, \cdots, n_k$, then the first degree congruence equations exactly has one solution, and

$$x \equiv M_1 M_1^{-} a_1 + M_2 M_2^{-} a_2 + \cdots + M_k M_k^{-} a_k(\bmod v)$$

2.2 Quadratic residues

Next is some talking about the solution of a Quadratic congruent equation.

$$x^2 \equiv a(\bmod n)$$

Suppose that $(a, n) = 1$, a is any integer and n is a natural number. Then a is called a quadratic residue $(\bmod n)$ if the congruence $x^2 \equiv a(\bmod n)$ is soluble; otherwise it is called a quadratic non-residue$(\bmod n)$.

Definition 2.5 (Legendre Symbol)

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & if(a, p) = 1 \text{ and } a \text{ is a quadratic residue} \mod p. \\ -1, & if(a, p) = 1 \text{ and } a \text{ is a quadratic non-residue} \mod p \\ 0, & p \mid a \end{cases}$$

Theorem 2.12 (Law of quadratic reciprocity)

If p, q are odd primes, then

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

Theorem 2.13 (Euler's criterion)

If p is an odd prime, then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p)$$

Property $\forall a, b \in \mathbb{Z}$,

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

Lemma 2.1 (Gauss' Lemma)

Suppose p is a prime, and $(a, p) = 1$. Further let a_j be the numerically residue of $aj(\mathrm{mod} p)$ for $j = 1, 2, \ldots$. Then Gauss's lemma states that

$$\left(\frac{a}{p} = (-1)^l\right)$$

where l is the number of $j \leq \frac{1}{2}(p-1)$ for which $a_j < 0$.

2.3 Practice