Review VI(Slides 312 - 351)

Modular Arithmetic

HamHam

University of Michigan-Shanghai Jiao Tong University Joint Institute

January 25, 2022

VE203 - Discrete Mathmatics

Modular Arithmetic

Definition

For $a, b \in \mathbb{Z}$, and $m \in \mathbb{N}\backslash\{0\}$ we say that a ***is congruent to*** b ***modulo*** m, writing

$$a \equiv b \pmod{m} \quad \text{iff} \quad m \mid (a-b)$$

The followings are equivalent:

- $a \equiv b \pmod{m}$
- $\underset{k\in\mathbb{Z}}{\exists} a = b + km$
- $a \bmod m = b \bmod m$

For any $n \in \mathbb{Z}$ $\equiv$ is an equivalence relation on $\mathbb{Z}$. We call such equivalence classes **congruence classes**, denoted as $a := [a]_\equiv$ for $a \in \mathbb{Z}$. The set of congruence classes is denoted as $\mathbb{Z}/n\mathbb{Z}$ in consistence with the notation in group theory.

Modular Arithmetic

Under a given modulo, the congruence map $a \to \bar{a}$ preserves the arithmetic of integers, that is

- $\overline{a+b} = \bar{a} + \bar{b}$
- $\overline{ab} = \bar{a} \cdot \bar{b}$

Or you may prefer to write:

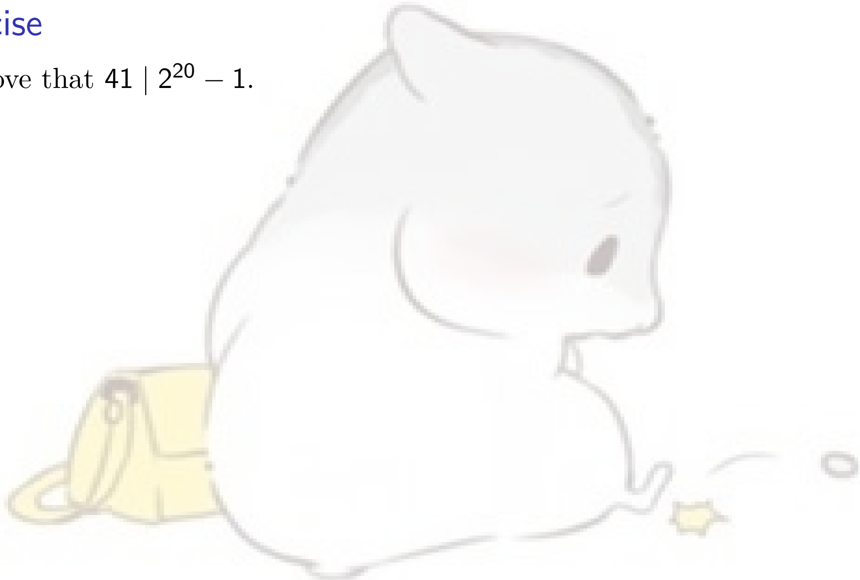
- $a + b \equiv (a \bmod m + b \bmod m) \pmod{m}$
- $a \cdot b \equiv (a \bmod m) \cdot (b \bmod m) \pmod{m}$

Thus the following two are groups:

- $(\mathbb{Z}/n\mathbb{Z}, +)$
- $(\{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n = 1)\}, \times)$ (Sometimes $(\mathbb{Z}/n\mathbb{Z}, \times)$ or $(\mathbb{Z}/n\mathbb{Z})^\times$ for short)

Exercise

1. Prove that $41 \mid 2^{20} - 1$.



Exercise

1. Prove that $41 \mid 2^{20} - 1$.

Solution:

This is equivalent to showing that

$$2^{20} - 1 \equiv 0 \pmod{41}.$$

We note that $2^5 = 32 \equiv -9 \pmod{41}$. Then

$$2^{20} = (2^5)^4 \equiv (-9)^4 \pmod{41}$$

But $(-9)^4 = 81 \cdot 81$ and $81 \equiv -1 \pmod{41}$. So

$$2^{20} \equiv (-1)^2 \equiv 1 \pmod{41}$$

Division in Modular Arithmetic

We have seen the addition and multiplication in modular arithemetic, what about division?

Theorem

Let $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{N}\backslash\{0\}$. Then

$$ac \equiv bc \pmod{m} \quad \Rightarrow \quad a \equiv b \pmod{m/d}$$

where $d = \gcd(c, m)$.

Proof

There exist integers r, s with $\gcd(r, s) = 1$ such that $c = rd, m = sd$. Insert them to the equation $ac - bc = k \cdot m$.

Modular Inverse

Definition

Let $a \in \mathbb{Z}$ and $m \in \mathbb{N} \backslash \{0, 1\}$ be given . Then an integer $a^{-1} \in \mathbb{Z}$ such that

$$aa^{-1} \equiv 1 \pmod{m}.$$

s said to be an inverse of a modulo m.

Theorem

Let $a \in \mathbb{N} \backslash \{0\}$ and $m \in \mathbb{N} \backslash \{0, 1\}$. If gcd(a, m) = 1, an inverse of a modulo m exists. This inverse is unique modulo m.

Proof

- Existence: Bézout's Theorem
- Uniqueness: Prove by contradiction

How to find the inverse

Solve $7x \equiv 1 \pmod{31}$ $\Leftrightarrow$ Solve $7 \cdot x - t \cdot 31 = 1$

Arithmetic Function

Definition

Arithmetic function, any mathematical function defined for integers (sometimes positive integers only) and dependent upon those properties of the integer itself as a number, in contrast to functions that are defined for other values (real numbers, complex numbers, etc.) and that involve various operations from algebra and calculus.

Example

- Euler's Totient Function $\varphi(n)$
- $\pi(x)$, number of primes no larger than x
- $\tau(a)$, number of positive factors of a
- $\sigma(a)$, sum of all positive factors of a
- Mobius Function $\mu(a) = \begin{cases} 1, & a = 1, \\ (-1)^r, & \text{product of } r \text{ different primes} \\ 0, & \text{divisible by a prime square} \end{cases}$

Multiplicative Function

Definition

A function $f : \mathbb{N}\backslash\{0\} \to \mathbb{N}\{0\}$ is multiplicative if $f(1) = 1$ and $f(m_1 m_2) = f(m_1) f(m_2)$ for $\gcd(m_1, m_2) = 1$.

Exercise

Check whether the followings are multiplicative functions:

- $f(n) = n^c$, where c is an arbitrary constant.
- $f(n) = [\text{For any integer } k > 1, k^2 \nmid n]$.
- $f(n) = c^k$, where k is the number of primes that divides n.
- The product of any two multiplicative functions.

Answer: True; False; True; True.

Comment. This does appear in the slides!

Exercise

2. Let $f(x)$ be a multiplicative function, and the standard decomposition for a is $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then

$$\begin{aligned}\sum_{d|a} f(d) &= \prod_{i=1}^{k} \left(1 + f(p_i) + f\left(p_i^2\right) + \cdots + f\left(p_i^{\alpha_i}\right)\right) \\ &= \prod_{i=1}^{k} \sum_{j=0}^{\alpha_i} f\left(p_i^j\right)\end{aligned}$$

Comment. It is easy to see that, $f(1)$ must be 1.

Proof

All the positive factor of a is

$$p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \beta_i = 0, 1, 2, \cdots, \alpha_i, i = 1, 2, \cdots, k$$

So that

$$\begin{aligned}
\sum_{d|a} f(d) &= \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \cdots \sum_{\beta_k=0}^{\alpha_k} f\left(p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}\right) \\
&= \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \cdots \sum_{\beta_k=0}^{\alpha_k} f\left(p_1^{\beta_1}\right) f\left(p_2^{\beta_2}\right) \cdots f\left(p_k^{\beta_k}\right) \\
&= \prod_{i=1}^{k} \left(f\left(p_i^0\right) + f\left(p_i\right) + f\left(p_i^2\right) + \cdots + f\left(p_i^{\alpha_i}\right)\right)
\end{aligned}$$

Euler's Totient Function

Definition

The Euler's Totient Function counts the number of positive integers less than n and relatively prime to n, i.e.

$$\varphi(n) = |\{k \in \mathbb{N} \mid \gcd(k,n) = 1, 1 \leq k \leq n\}| = |(\mathbb{Z}/n\mathbb{Z})^*|$$

Properties:

- $\varphi(p) = p - 1$
- $\varphi(p^k) = p^k - p^{k-1} (k \geq 1)$
- $\varphi(mn) = \varphi(m) \cdot \varphi(n)$, if $\gcd(m,n) = 1$
- $\varphi(n) = \sum_{d|n} \varphi(d)$
- $\varphi(a) = \varphi\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = \prod_{i=1}^{k} (p_i - 1) p_i^{\alpha_i - 1}$
- $\varphi(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$

Exercise

This is challenging!

3. Let $S_{p,q} = \{f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} \mid f \text{ is a group homomorphism}\}$. Given p, q primes, $p < q$, then

(A) $f(1) = 1$ if $f \in S_{p,q}$

(B) f is an isomorphism if $f \in S_{p,q}$

(C) $|S_{p,q}| \leq |S_{q,p}|$

(D) $|S_{p,q}| = \varphi(q)^{\varphi(p)}$

Answer: C

Euler's Theorem

Theorem (Euler)

For $m \in \mathbb{N} \backslash \{0\}$ and $a \in \mathbb{Z}$ such that $\gcd(a, m) = 1$,

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

Proof

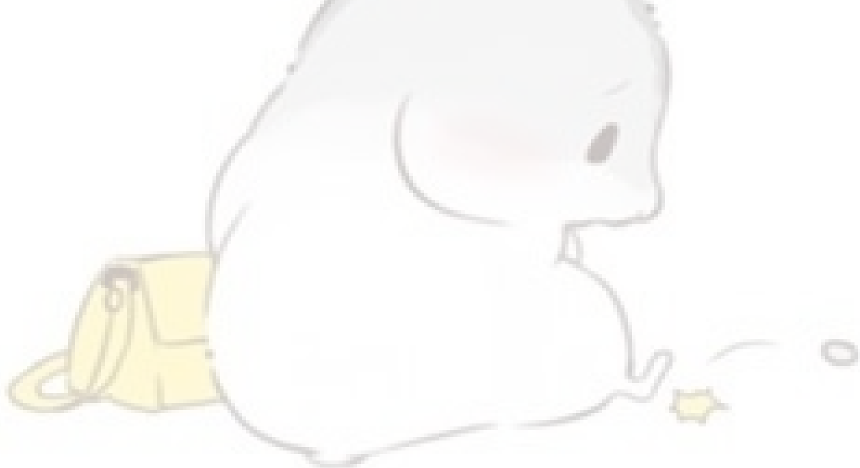
Let $G = (\mathbb{Z}/m\mathbb{Z})^*$, then $\forall a \in G$, $a^{|G|} = 1_G$.

Remark

When $m \in \mathbb{P}$, this becomes Fermat's Little Theorem.

Exercise

4. Given $a, n \in \mathbb{N}$ and $a, n > 1$, show that $n \mid \varphi(a^n - 1)$.



Exercise

4. Given $a, n \in \mathbb{N}$ and $a, n > 1$, show that $n \mid \varphi(a^n - 1)$.

Solution 1:

Let $m = a^n - 1$, consider the multiplicative group $G = (\mathbb{Z}/m\mathbb{Z})^\times$.

First we prove the order of a is n. Indeed, $a^n \equiv 1 \pmod{m}$ and $a^x \not\equiv 1 \pmod{m}$ for $1 < x < m$ since $1 < a^x < a^n = m$.

According to Lagrange's theorem, therefore the order of a divides the order of G, that is, $n \mid \varphi(a^n - 1)$.

Solution 2:

$$\left.\begin{array}{r} m = a^n - 1 \Rightarrow a^n \equiv 1 \pmod{m} \\ \text{Euler} \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m} \end{array}\right\} \Rightarrow n \mid \varphi(m) \text{ (why?)}$$

Fermat's Little Theorem

Theorem

Given $a \in \mathbb{Z}$ and $p \in \mathbb{P}$, such that $(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}$$
$$a^{p} \equiv a \pmod{p}$$

Proof

Induction on a.

Fermat Primality Test

- If $2^n \not\equiv 2 \pmod{n}$, then n is NOT prime.
- If $2^n \equiv 2 \pmod{n}$, then n is PROBABLY prime.

Fast Exponentiation

Express power in binary and play with your CASIO 991CN.

Another Proof

Here is another proof of Fermat's Little Theorem.

Consider the set $S = \{a, 2a, \cdots, (p-1)a\}$. For any ma, na in S, there doesn't exist $ma \equiv na \pmod{p}$. (Why?) Therefore

$$S \bmod p = \{0 \leqslant k \leqslant p-1 | ma \equiv k \pmod{p}, ma \in S\} = \{1, 2, \cdots, p-1\}$$

Then,

$$a \cdot 2a \cdots (p-1)a \equiv (p-1)! \pmod{p}$$

which implies

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Since $\gcd((p-1)!, p) = 1$, we conclude $a^{p-1} \equiv 1 \pmod{p}$.

Exercise

Prove Euler's Theorem by considering

$$S = \{ka | \gcd(k, n) = 1, 1 \leqslant k \leqslant n\}$$

Wilson's Theorem

Theorem (Wilson)

Let $p \in \mathbb{N}$ be prime. Then

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof:

Key idea: find the inverse and match in pair.

The inverse a^{-1} modulo p of a exists and is unique modulo p,

$$a^{-1}a \equiv 1 \pmod{p}$$

Proof

We first show that $a = a^{-1}$ if and only if $a = 1$ or $a = p - 1$.

It is easily checked that

$$1 \cdot 1 \equiv 1 \pmod{p} \quad \text{and} \quad (p-1)^2 \equiv 1 \pmod{p}$$

Now suppose that $a^2 \equiv 1 (\bmod p)$. Then

$$(a-1)(a+1) \equiv 0 \pmod{p}$$

Since p is prime, this implies $a - 1 \equiv 0$ or $a + 1 \equiv 0 \pmod{p}$. Hence, either $a = 1$ or $a = p - 1$.

Proof (Cont.)

Next, consider the remaining $p - 3$ integers

$$2, 3, \dots, p - 2$$

Since the inverse a^{-1} of a is unique, it follows that these numbers can be grouped into pairs a, a^{-1} where $a^{-1} \neq a$ and $a^{-1}a \equiv 1 \pmod{p}$. Therefore,

$$(p-2)! = 2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$$

Multiplying by $p - 1$,

$$(p-1)! \equiv p - 1 \equiv -1 \pmod{p}$$

which is what we wanted to show.

Chinese Remainder Theorem

This is from Xue Runze.

Lemma

For $\gcd(m,n)=1$, we have $(\mathbb{Z}/mn\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$

Theorem (Chinese Remainder Theorem)

For $\gcd(m_i, m_j) = 1$ for all $i \neq j$, we have

$$\mathbb{Z}/\left(\prod_{i=1}^{n} m_i\right)\mathbb{Z} \cong \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$$

and

$$\left(\mathbb{Z}/\left(\prod_{i=1}^{n} m_i\right)\mathbb{Z}\right)^{\times} \cong \prod_{i=1}^{n} (\mathbb{Z}/m_i\mathbb{Z})^{\times}$$

Exercise

It's better to do an exercise and make friends with CASIO 991CN.

5. Solve the following system of linear Diophantine equations,

$$x \equiv 3 \pmod{8}, \quad x \equiv 1 \pmod{15}, \quad x \equiv 11 \pmod{20}$$

Comment. Please note that $\{m_i\}_{i=1}^r$ should be **pairwise coprime** before you apply the formula.

Recipe

$$x \equiv \sum_{i=1}^{r} a_i y_i \pmod{m}$$

where $m = \prod_{i=1}^r m_i$ and $y_i = (m/m_i)^{\varphi(m_i)} \equiv \delta_{ij} \pmod{m_j}$.

RSA Cryptography

For your better preparation for the exam, we here omit the technical details and gives the operation steps only.

- The **public key** to be published is a pair of positive integers $(n := pq, E)$ where $p, q \in \mathbb{P}$ and $p \neq q$, and $E < \varphi(n)$, $\gcd(E, \varphi(n))$.
- The **encryption function** is

$$y = e(x) := x^E \pmod n$$

- The private key $D := E^{-1} \bmod \varphi(n)$. The **decryption function** is therefore

$$d(y) := y^D = x^{ED} = x \pmod n$$

- Be careful and play with CASIO 991CN.

Distribution of Primes (Part II)

Last time we proved two lemmas:

Lemma 1

Let n be any positive integer, set

$$N = \frac{(2n)!}{(n!)^2}$$

then

$$(\pi(2n) - \pi(n)) \ln n \le \ln N \le \pi(2n) \ln(2n).$$

Lemma 2

For the same n, N defined in Lemma 1, we have

$$n \ln 2 \le \ln N \le 2n \ln 2.$$

Distribution of Primes (Part II)

Now, it's time to prove the inequality.

Proposition

Let $x \geq 2$, then

$$0.2\frac{x}{\ln x} \leq \pi(x) \leq 5\frac{x}{\ln x}$$

Proof: (Left)

If $x \geq 6$, let $n = \lfloor x/2 \rfloor$, then $x \geq 2n, n > x/3$. From Lemma 1,2 we immediately obtain that

$$\pi(x)\ln x \geq \pi(2n)\ln(2n) \geq \ln N \geq n\ln 2 > \frac{\ln 2}{3} \cdot x > 0.2x$$

Considering that the maximum of $x/\ln x$ on the interval $[2, 6]$ is $6/\ln 6$, so when $2 \leq x \leq 6$,

$$0.2\frac{x}{\ln x} \leq 0.2\frac{6}{\ln 6} < 1 = \pi(2) \leq \pi(x).$$

Proof (Right)

From Lemma 1,2, we know

$$(\pi(2n)-\pi(n))\ln(n) \leq \ln N \leq 2n\ln 2.$$

Plug in $n=2^r$,

$$r\left(\pi\left(2^{r+1}\right)-\pi\left(2^r\right)\right) \leq 2^{r+1}.$$

Since $\pi(2^{r+1}) \leq 2^r$,

$$(r+1)\pi\left(2^{r+1}\right)-r\pi\left(2^r\right) \leq 2^{r+1}+\pi\left(2^{r+1}\right) \leq 3\cdot 2^r$$

For any positive integer m, let $r=0,1,\cdots,m-1$, we can obtain m inequalities.

Proof (Right)

Add the above m inequalities together,

$$m\pi\left(2^m\right) \leq 3(1+2+\cdots+2^{m-1}) < 3\times 2^m.$$

When $x \geq 2$, there exists a unique positive integer m , such that $2^{m-1} \leq x < 2^m$, so $1/m < \ln 2/\ln x$. We get

$$\pi(x) \leq \pi\left(2^m\right) \leq \frac{1}{m}\cdot 3\cdot 2^m \leq 6\ln 2\cdot\frac{x}{\ln x} \leq 5\frac{x}{\ln x}$$

This complete out proof.

Corollary

Almost all the numbers are composite, namely

$$\lim_{x\to\infty}\frac{\pi(x)}{x} = 0.$$

More Result

Theorem

A more advanced result, the prime number theorem

$$\lim_{x\to\infty}\frac{\pi(x)}{\frac{x}{\ln x}}=1.$$

The Best result so far

Let

$$li(x):=\int_2^x\frac{\mathrm{d}t}{\ln t}$$

Then

$$|\pi(x)-li(x)|\leq Bxe^{-A(\ln x)3/5\times(\ln\ln x)-3/5}$$

A Guess

$$|\pi(x)-li(x)|\leq Bx^{\frac{1}{2}+\varepsilon}$$

Exercise

6. Let p_n be the n-th prime. Prove that: there exists two positive numbers B_1, B_2, such that

$$B_a n \ln n \leq p_n \leq B_2 n \ln n$$

Reference

- Example From Horst's Slides FA2021.
- Exercises from 2021-Fall-Ve203 Mid_2 Exam.
- Exercises from 2019-Fall-Ve203 TA Yan Xinyu.
- Contents from 2021-Fall Mid_2_RC by Xue Runze.
- Yan Shijian, etc. *Basic Number Theory*, fourth edition. Beijing: Higher Education Press, 2020.5 print.