Discrete Mathematics Recitation Class

Tianyu Qiu

University of Michigan - Shanghai Jiaotong University

Joint Institute

Summer Term 2020

Contents

Prime Numbers

Definition(P193)

1. *prime*
2. *composite*

Theorem

(P193) Let $p \in \mathbb{N} \setminus \{0, 1\}$ *and* $a, b \in \mathbb{Z}$*. If* p *is prime and* $p \mid ab$*, then* $p \mid a$ *or* $p \mid b$*.*

Corollary

(P193) Let $p \in \mathbb{N} \setminus \{0, 1\}$ *and* $a_1, \cdots, a_n \in \mathbb{Z}$*. If* p *is prime and* $p \mid \prod_{k=1}^{n} a_k$*, then* $p \mid a_k$ *for some* k *with* $1 \leq k \leq n, k \in \mathbb{Z}$*.*

Corollary

(P194) Let $p, q_1, \cdots, q_n \in \mathbb{N} \setminus \{0, 1\}$*. If* p *is prime and* $p \mid \prod_{k=1}^{m} q_n$*, then* $p = q_k$ *for some* k *with* $1 \leq k \leq n, k \in \mathbb{Z}$*.*

Theorems of Prime Numbers

Theorem (Fundamental Theorem of Arithmetic)

(P195) Every $n \in \mathbb{N} \setminus \{0, 1\}$ is prime or the product of primes. This product is unique, apart from the order in which the primes occur.

Corollary

(P196) Any $n \in \mathbb{N} \setminus \{0, 1\}$ can be written in the canonical from

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

where $p_1 < \cdots < p_r$ are prime numbers and $k_1, \cdots, k_r \in \mathbb{N} \setminus \{0\}$

Theorem (The Sieve of Eratosthenes)

(P197) If n is a composite integer, then n has a prime divisor whose square is not greater than n.

Theorem

(P199) There are infinitely many primes.

Congruency

Definition(P204)
congruency: a is congruent to b modulo m, writing $a \equiv b \pmod{m}$ if and only if $m \mid (a-b)$

Lemma

(P204) Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N} \setminus \{0\}$. Then

$$a \equiv b(\ mod \ m) \Leftrightarrow \underset{k \in \mathbb{Z}}{\exists} \ a = b + km$$

Theorem

(P205) Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N} \setminus \{0\}$. Then

$$a \equiv b(\ mod \ m) \Leftrightarrow a \ mod \ m = b \ mod \ m$$

Congruency Class

Definition(P206-P207)

1. *congruency classes*: $\mathbb{Z}_m = \{[0]_m, [1]_m, \cdots, [m-1]_m\}$
2. *addition*: $[a]_m + [b]_m = [a+b]_m$
3. *multiplication*: $[a]_m \cdot [b]_m = [a \cdot b]_m$

Lemma

(P208) Let $a, \tilde{a}, b, \tilde{b} \in \mathbb{Z}$ *and* $m \in \mathbb{N} \setminus \{0\}$. *If* $a \equiv \tilde{a} \bmod m$ *and* $b \equiv \tilde{b} \bmod m$, *then*

$$a + b = \tilde{a} + \tilde{b} \bmod m, \qquad ab \equiv \tilde{a}\tilde{b} \bmod m$$

Corollary

(P209) Let $a, b \in \mathbb{Z}$ *and* $m \in \mathbb{N} \setminus \{0\}$. *Then*

$$a + b \equiv (a \bmod m + b \bmod m) \bmod m$$
$$ab \equiv (a \bmod m)(b \bmod m) \bmod m$$

Division in Modular Arithmetic

Theorem

(P213) Let $a, b, c \in \mathbb{Z}$ *and* $m \in \mathbb{N} \setminus \{0\}$. *Then*

$$ac \equiv bc \bmod m$$

implies

$$a \equiv b \bmod m/d$$

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

Corollary

(P214) Let $a, b, c \in \mathbb{Z}$ *and* $m \in \mathbb{N} \setminus \{0\}$ *and* $gcd(c, m) = 1$. *Then*

$$ac \equiv bc \bmod m$$

implies

$$a \equiv b \bmod m$$

Modular Inverse

Definition(P215)
inverse of a modulo m

Theorem
(P215) Let $a \in \mathbb{N} \backslash$ *and* $m \in \mathbb{N} \setminus \{0,1\}$. *If* $gcd(a,m) = 1$, *an inverse of a modulo m exists. This inverse is unique modulo m.*

Theorem
(P217) The partition $\mathbb{Z}_p$ *is a field if and only if p is a prime number.*

Finding Modular Inverse

Theorem

Define that $\mathbb{Z}_m^* = \{[k]_m | \exists x \in \mathbb{Z}(kx \equiv 1 \ mod \ m)\}$, then $(\mathbb{Z}_m^*, \cdot)$ is a group.

Proof.

1. Show that the group operation is closed on the set.
2. Show that the unit element exists.
3. Show that the inverse exists.

$\square$

All the representatives in $\mathbb{Z}_m^*$ and m are relatively prime.

Cayley Table

Table: Cayley Table for modulo 6

$\otimes_6$	$[1]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[5]_6$
$[5]_6$	$[5]_6$	$[1]_6$

Table: Cayley Table for modulo 12

$\otimes_{12}$	$[1]_{12}$	$[5]_{12}$	$[7]_{12}$	$[11]_{12}$
$[1]_{12}$	$[1]_{12}$	$[5]_{12}$	$[7]_{12}$	$[11]_{12}$
$[5]_{12}$	$[5]_{12}$	$[1]_{12}$	$[11]_{12}$	$[7]_{12}$
$[7]_{12}$	$[7]_{12}$	$[11]_{12}$	$[1]_{12}$	$[5]_{12}$
$[11]_{12}$	$[11]_{12}$	$[7]_{12}$	$[5]_{12}$	$[1]_{12}$

Linear Congruence

Definition(P219)

linear congruence: $ax \equiv \mod m$ for unknowns $x \in \mathbb{Z}$.

Theorem

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N} \setminus \{0\}$ and $d = gcd(a, m)$. The linear congruence $ax \equiv \mod m$ has a solution if and only if $d|b$. In this case, it has d solutions that are mutually incongruent modulo m.

Proof.

1. existence: just the same as Linear Diophantine Equations
2. d mutually incongruent solutions: proof by contradiction
3. Show all the other solutions are congruent with these d solutions.

Corollary

(P224) Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N} \setminus \{0\}$ and $gcd(a, m) = 1$. Then the linear congruence $ax \equiv \mod m$ has a unique solution modulo m.

Chinese Remainder Theorem (P227-P230)

Theorem (Chinese Remainder Theorem)

Let $m_1, \ldots, m_n \in \mathbb{N} \setminus \{0\}$ *be pairwise relatively prime and let* $a_1, \ldots, a_n \in \mathbb{Z}$ *. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 (\bmod m_1) \\ x &\equiv a_2 (\bmod m_2) \\ &\vdots \\ x &\equiv a_n (\bmod m_n) \end{aligned}$$

has a unique solution $(\bmod m)$ *where* $m = m_1 \cdots m_n$.

Chinese Remainder Theorem (P227-P230)

Proof.

We first prove the existence of a solution. For all $1 \leq k \leq n$, define

$$M_k = \frac{m}{m_k} = \prod_{i \neq k} m_i$$

Note that since $m_1, \ldots, m_n$ are pairwise relatively prime, it follows that for all $1 \leq k \leq n, \gcd(m_k, M_k) = 1$. Therefore for all $1 \leq k \leq n$ $[M_k]_{m_k} \in \mathbb{Z}^*_{m_k}$ and there exists $y_k \in \mathbb{Z}$ such that

$$[M_k y_k]_{m_k} = [M_k]_{m_k} \cdot [y_k]_{m_k} = [1]_{m_k} \text{ or } M_k y_k \equiv 1 \pmod{m_k}$$

Chinese Remainder Theorem (P227-P230)

Proof(Continued).

Let

$$x = \sum_{k=1}^{n} a_k M_k y_k$$

since for all $1 \leq i, j \leq n$, if $i \neq j$, then $M_i \equiv 0 \pmod{m_j}$, it follows that x is a solution to (11).

We now turn to showing uniqueness. Let $x, x' \in \mathbb{Z}$ be such that for all $1 \leq k \leq n$,

$$x \equiv a_k \equiv x' \pmod{m_k}$$

We will show that x and x' must be congruent $(\operatorname{mod} m)$. Now, for all $1 \leq k \leq n$, $m_k | (x - x')$. An elementary induction argument applied to one of the consequences of Bézout's Lemma that we proved shows that since for all $1 \leq i, j \leq n$ with $i \neq j, \gcd(m_i, m_j) = 1$

Chinese Remainder Theorem (P227-P230)

Proof(Continued).

$$m = m_1 \cdots m_n \mid (x - x')$$

This shows that

$$x \equiv x' \pmod{m}$$

$\square$

Useful Conclusion

Given that $a, b, c, d \in \mathbb{N} \setminus \{0\}$, b, c, d are mutually relatively prime, then:

$$\begin{cases} dx \equiv a \pmod{b} \\ dx \equiv a \pmod{c} \end{cases} \Leftrightarrow dx \equiv a \pmod{bc}$$

Exercises

1.

$$15x \equiv 2 \bmod 7$$
$$12x \equiv 3 \bmod 5$$
$$20x \equiv 6 \bmod 13$$

2.

$$7x \equiv 3 \bmod 30$$
$$11x \equiv 7 \bmod 24$$
$$13x \equiv 11 \bmod 20$$

Solutions

1. Manipulate the oringinal equation(s) to the form that Chinese Remainder Theorem is applicable.

$$15x \equiv 2 \bmod 7 \;\Leftrightarrow\; x \equiv 2 \bmod 7$$
$$12x \equiv 3 \bmod 5 \;\Leftrightarrow\; 2x \equiv 3 \bmod 5 \Leftrightarrow x \equiv 4 \bmod 5$$
$$20x \equiv 6 \bmod 13 \;\Leftrightarrow\; x \equiv 12 \bmod 13$$

2. Check whether solution(s) exists.
3. Apply Chinese Remainder Theorem:

$$\begin{aligned} M_1 &= 65, & y_1 &= 4 \\ M_2 &= 91, & y_2 &= 1 \\ M_3 &= 35, & y_2 &= 3 \end{aligned}$$

Then we have

$$x_0 = 2 \cdot 65 \cdot 4 + 4 \cdot 91 \cdot 1 + 12 \cdot 35 \cdot 3 = 2144$$
$$x = 2144 + 455t, t \in \mathbb{Z}$$

Solutions

- $$\begin{aligned}
7x \equiv 3 \bmod 30 \;\Leftrightarrow\; & 7x \equiv 3 \bmod 5 \;\Leftrightarrow\; 2x \equiv 3 \bmod 5 \\
& 7x \equiv 3 \bmod 6 \;\Leftrightarrow\; x \equiv 3 \bmod 6 \\
11x \equiv 7 \bmod 24 \;\Leftrightarrow\; & 11x \equiv 7 \bmod 4 \;\Leftrightarrow\; 3x \equiv 3 \bmod 4 \\
& 11x \equiv 7 \bmod 6 \;\Leftrightarrow\; 5x \equiv 1 \bmod 5 \\
13x \equiv 11 \bmod 20 \;\Leftrightarrow\; & 13x \equiv 11 \bmod 4 \;\Leftrightarrow\; x \equiv 3 \bmod 4 \\
& 13x \equiv 11 \bmod 5 \;\Leftrightarrow\; 3x \equiv 1 \bmod 5
\end{aligned}$$
- This series has no solutions.