Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

March 1, 2023

What we have seen last week

Polynomials modulo p

- Division of polynomials
- Monic polynomials
- Greatest common divisor and Least common multiple
- (Euclidean) division algorithm
- Units and irreducible polynomials
- Unique prime factorization
- Roots and degree

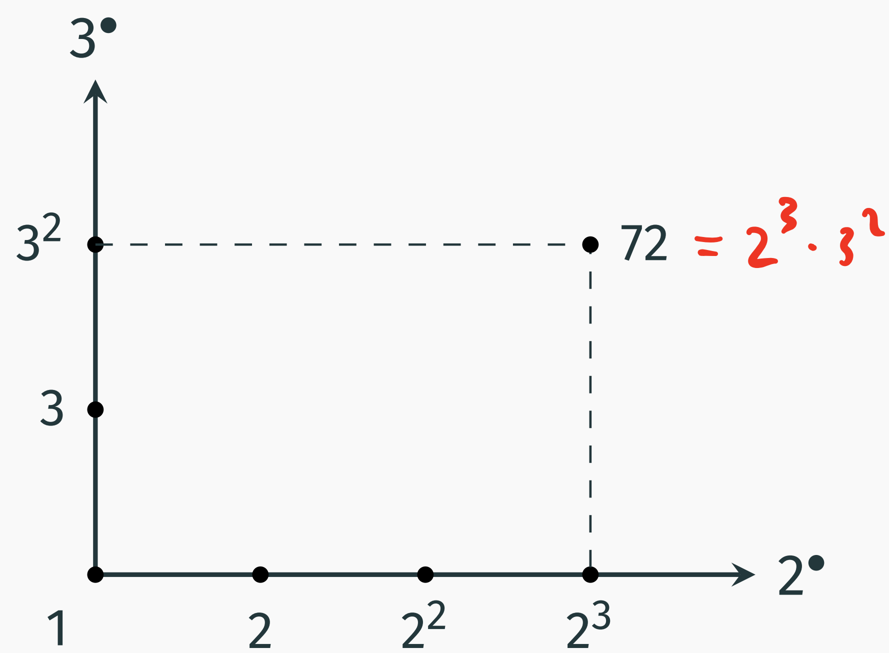
Today's topics

- Chinese Remainder Theorem

Part VII

Assembling modular worlds

Each modular world tells partial information of the integer world.



$(3, 2, 0, 0, \dots)$

$v_2 \quad v_3 \quad v_5 \quad \dots$

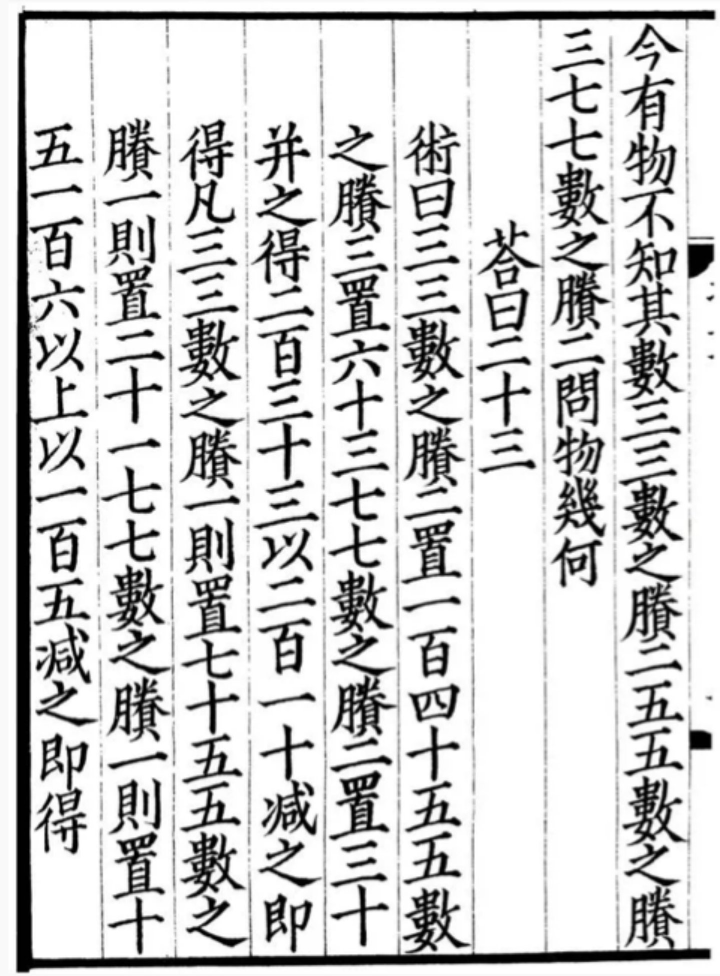
Chinese Remainder Theorem

There are certain things whose number is unknown

Chinese Remainder Theorem arises from a puzzle in the 3rd-century book *Sun-tzu Suan-ching* by the Chinese mathematician *Sun-tzu*.

There are certain things whose number is unknown.
If count them by 3s we have 2 left over.
If count them by 5s we have 3 left over.
If count them by 7s we have 2 left over.
How many things are there?

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases} \Rightarrow x = ?$$



今有物不知其數三三數之賸二五五數之賸
三七七數之賸二問物幾何
荅曰二十三
術曰三三數之賸二置一百四十五五數
之賸三置六十三七七數之賸二置三十
并之得二百三十三以二百一十減之即
得凡三三數之賸一則置七十五五數之
賸一則置二十一七七數之賸一則置十
五一百六以上以一百五減之即得

There are certain things whose number is unknown

The original answer says:

- count them by 3s and left over 2 $\Longrightarrow$ Put number 140. ?
- count them by 5s and left over 3 $\Longrightarrow$ Put number 63. ?
- count them by 7s and left over 2 $\Longrightarrow$ Put number 30. ?
- Their total gives 233.
- Subtract 210 from it, we get the final 23. $233 \equiv 23 \mod 105$

common mutiple of 3, 5, 7

There are certain things whose number is unknown

Question

There are certain things whose number is unknown. If count them by 3s we have 2 left over. If count them by 5s we have 3 left over. How many things are there?

We first translate the system of congruence equations into a system of linear equations:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases} \quad \Rightarrow \quad \begin{cases} x = 2 + 3y \\ x = 3 + 5z \end{cases}$$

The system of linear equations then can be organized into a linear Diophantine equation:

$$3y - 5z = 1.$$

There are certain things whose number is unknown

By theorem 3.5, we have the following general solution

$$\begin{cases} y = 2 + 5m \\ z = 1 + 3m \end{cases}$$

Substituting them into the linear equations, we get

$$x = 8 + 15m.$$

Namely, $x \equiv 8 \pmod{15}$.

We may generalize the previous into the following.

Theorem 19.1 (Chinese remainder theorem, binary version)

Suppose m and n are two coprime moduli. Then there is a bijection

$$f : \mathbb{Z}/m \times \mathbb{Z}/n \longrightarrow \mathbb{Z}/mn$$

such that whenever $f(a, b) = c$, we have

$$\left\{ x \in \mathbb{Z} \;\middle|\; \begin{array}{l} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{array} \right\} = \left\{ x \in \mathbb{Z} \;\middle|\; x \equiv c \pmod{mn} \right\}.$$

Proof. We first translate the system of congruence equations into a system of linear equations:

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \implies \begin{cases} x = a + my \\ x = b + nz \end{cases}$$

The system of linear equations then can be organized into a linear Diophantine equation:

$$my - nz = b - a.$$

Note that any solution of this equation satisfies

$$a + my = b + nz.$$

Let c be the natural representative of this constant modulo mn.

Chinese Remainder Theorem

Since m and n are coprime, we have a specific solution (y_0, z_0) of the above equation. Then by theorem 3.5, we have the following general solution

$$\begin{cases} y = y_0 + nt \\ z = z_0 + mt \end{cases}$$

Substituting them into the linear equations, we get

$$x = a + my_0 + mnt = b + nz_0 + mnt \equiv c \pmod{mn}.$$

$(a, b) \longmapsto c$

We thus get a map $f : \mathbb{Z}/m \times \mathbb{Z}/n \longrightarrow \mathbb{Z}/mn$ satisfying the requirements. To see it is a bijection, consider the following inverse map of it:

$$[c]_{mn} \longmapsto ([c]_m, [c]_n). \qquad \square$$

What about multi-variables version?

$\operatorname{lcm}_{i \in I}(m_i) = \prod_{i \in I} m_i$

Theorem 19.2 (Chinese remainder theorem)

Suppose m_i $(i \in I)$ be moduli which are coprime to each other. Let M be the product of them. Then there is a bijection

$$f : \prod_{i \in I} \mathbb{Z}/m_i \longrightarrow \mathbb{Z}/M$$

such that whenever $f((a_i)_{i \in I}) = A$, we have

$$\left\{ x \in \mathbb{Z} \,\middle|\, x \equiv a_i \pmod{m_i}, \forall i \in I \right\} = \left\{ x \in \mathbb{Z} \,\middle|\, x \equiv A \pmod{M} \right\}.$$

Proof. By theorem 19.1, we can always replace two congruence equations by a single one with the modulus being the product of former. Apply this to an induction on $|I|$, we get the theorem. $\square$

Example 19.3

For the original "things whose number is unknown" problem, we have

$$\begin{cases} \boxed{\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \end{aligned}} \\ x \equiv 2 \pmod{7} \end{cases} \Rightarrow \begin{cases} \boxed{x \equiv 8 \pmod{15}} \\ x \equiv 2 \pmod{7} \end{cases} \Rightarrow x \equiv 23 \pmod{105}.$$

Chinese Remainder Theorem

In what follows, we will explain the original method in *Sun-tzu Suan-ching* and generalize it into a proof of theorem 19.2.

- count them by $\overset{m_i}{3}$s and left over $\overset{a_i}{2}$ $\Rightarrow$ Put number 140.
- count them by 5s and left over 3 $\Rightarrow$ Put number 63.
- count them by 7s and left over 2 $\Rightarrow$ Put number 30.
- Their total gives 233. $M_i N_i + m_i n_i = 1$
- Subtract 210 from it, we get the final 23.

m_i	M_i	a_i	N_i	n_i	$a_i M_i N_i$
3	35	2	2	-23	140
5	21	3	1	-4	63
7	15	2	1	-2	30

M_i = prod of moduli other than m_i

Proof. (Of 19.2) Let's construct the map $f : \prod_{i \in I} \mathbb{Z}/m_i \longrightarrow \mathbb{Z}/M$.

First, let $M_i = \frac{M}{m_i}$. By lemma 5.5, each M_i is coprime to m_i. Therefore, by Bézout's identity, there exist integers N_i and n_i such that

$$M_i N_i + m_i n_i = 1.$$

Then the map f maps $([a_i]_{m_i})_{i \in I}$ to the congruence class of

$$\sum_{i \in I} \boxed{a_i M_i N_i} \pmod{M}.$$

Note that $m_i \mid M_j$ $(i \neq j)$

$a_i M_i N_i \equiv a_i (M_i N_i + m_i n_i)$

$\equiv a_i \mod m_i$

It is straightforward to verify the requirements of f and the inverse map of f is given by $[A]_M \mapsto ([A]_{m_i})_{i \in I}$. $\square$

$$\begin{cases} x \equiv a_i \mod m_i \\ \cdots \end{cases} \Rightarrow x \equiv \sum_i a_i M_i N_i \mod M$$

Theorem 19.4 (Chinese remainder theorem, abstract version)

Suppose m_i $(i \in I)$ be moduli which are coprime to each other. Let M be the product of them. Then there is an isomorphism (bijective map preserving the structures)

$$f\colon \prod_{i\in I} \mathbb{Z}/m_i \longrightarrow \mathbb{Z}/M.$$

Here the ring structure (i.e. addition, multiplication, and their neutral elements) on the product $\prod_{i\in I} \mathbb{Z}/m_i$ is defined term wise.

Equivalently, the theorem states that the natural reduction map

$$\mathbb{Z}/M \longrightarrow \prod_{i\in I} \mathbb{Z}/m_i \colon [A]_M \mapsto ([A]_{m_i})_{i\in I}$$

is an isomorphism.

Proof. We first verify that the natural reduction map preserves the structures.

- $[A]_M + [B]_M = [A+B]_M \mapsto ([A+B]_{m_i})_{i\in I} = ([A]_{m_i})_{i\in I} + ([B]_{m_i})_{i\in I}$.
- $[A]_M \cdot [B]_M = [AB]_M \mapsto ([AB]_{m_i})_{i\in I} = ([A]_{m_i})_{i\in I} \cdot ([B]_{m_i})_{i\in I}$.
- $[0]_M \mapsto ([0]_{m_i})_{i\in I}$ and $[1]_M \mapsto ([1]_{m_i})_{i\in I}$.

Next, we show that the natural reduction map is injective. For this, we first note that the only preimage of $([0]_{m_i})_{i\in I}$ is $[0]_M$. Indeed, if $[A]_M$ is preimage of $([0]_{m_i})_{i\in I}$, then we have $m_i \mid A$. Since m_i are coprime to each other, by lemma 5.5, their product M also sivides A. Namely, $[A]_M = [0]_M$.

Finally, we conclude that the natural reduction map is bijective since it is an injection between two sets of the same size. □

Corollary 19.5

The Euler's totient φ is a multiplicative function.

Proof. The isomorphism on the left induces one on the right

$$\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n \qquad \Longrightarrow \qquad \Phi(mn) \cong \Phi(m) \times \Phi(n).$$

This is because if a is invertible modulo mn, then it is also invertible modulo m. $\square$

The power of "Abstract Algebra"

$$\mathbb{Z}/M \longrightarrow \prod_i \mathbb{Z}/m_i$$

Solve $f(T) \equiv 0 \bmod M$ $\xrightarrow{\text{nat. red}}$ Solve $f(T) \equiv 0 \bmod m_i$ $(\forall i)$

$$[X]_M \xleftarrow{f} \left([x_i]_{m_i}\right)_i$$

$$M = \prod_p p^{v_p(M)}$$