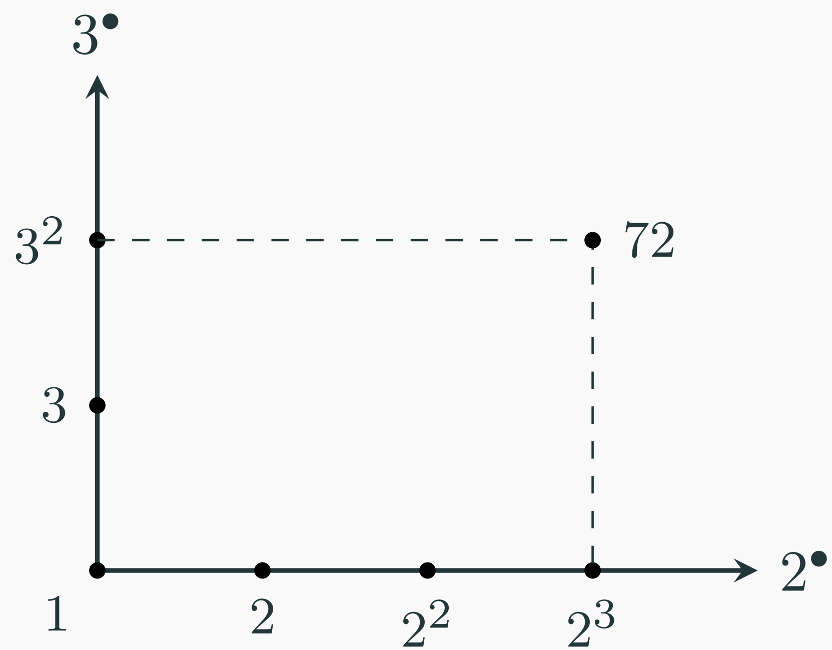
Part VI

Assembling modular worlds

Each modular world tells partial information of the integer world.

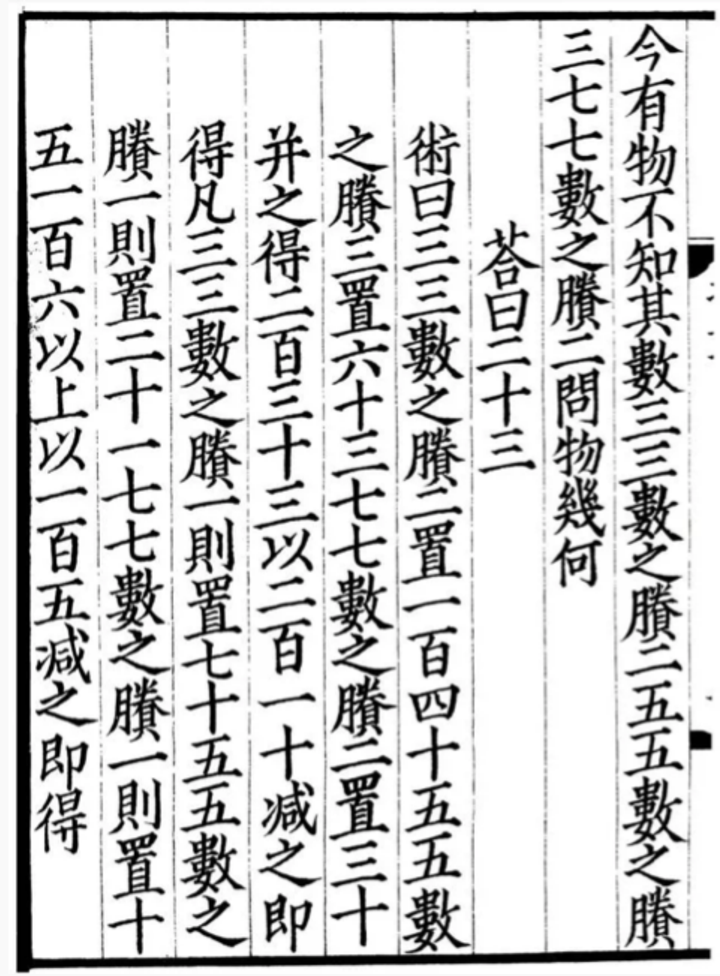


Chinese Remainder Theorem

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 $2 \Rightarrow$ 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.
- Subtract 210 from it, we get the final 23.

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:

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

By theorem 1.4.2, 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 6.1.1 (Chinese remainder theorem, binary version)

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

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

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

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

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

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

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

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

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

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

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.

Since m and n are coprime, we have a specific solution (y_0, z_0) of the above equation. Then by theorem 1.4.2, we have the following general solution

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

Since m and n are coprime, we have a specific solution (y_0, z_0) of the above equation. Then by theorem 1.4.2, 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

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

Now, we get a map $f\colon \mathbb{Z}/m \times \mathbb{Z}/n \longrightarrow \mathbb{Z}/mn$ satisfying the requirements. To see it is a bijection, consider the inverse map of it given by the following rule:

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

This finishes the proof. $\square$