Unit 4
The Chinese Remainder Theorem
中国剩余定理


孫子算經卷上

唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勅注釋

度之所起起於忽欲知其忽蠛吐絲爲忽十忽爲一絲十絲爲一毫十毫爲一氂十氂爲一分十分爲一寸十寸爲一尺十尺爲一丈十丈爲一引五十尺爲一端四十尺爲一疋六尺爲一步二百四十步爲一畝三百步爲一里

稱之所起起於黍十黍爲一累十累爲一銖二十四銖爲一兩十六兩爲一斤三十斤爲一鈞

Motivation

QUESTION

What should be the minimal length of the “magic word” if we wish to use 13 cards instead of 4?

$$\begin{cases} a+b \equiv -1[m] \\ a+b \equiv -1[m-1] \\ a+b \equiv -1[m-2] \end{cases} \Leftrightarrow \begin{cases} x \equiv -1[13] \\ x \equiv -1[12] \\ x \equiv -1[11] \end{cases} \qquad (x = a+b)$$

$$13 \times 12 \times 11 - 1 = 1715$$

The Chinese Remainder Theorem

QUESTION (Sun Tze Suan Ching, around 400 B. C.)

"We have a number of things, but we do not know exactly how many.

- **If we count them by threes we have two left over.**
- **If we count them by fives we have three left over.**
- **If we count them by sevens we have two left over.**

How many things are there?" (Quoted from Sun Tze Suan Ching).

$$\text{Find } x \in \mathbb{Z}\text{:} \quad \begin{cases} x \equiv 2[3] \\ x \equiv 3[5] \\ x \equiv 2[7] \end{cases}$$

The Chinese Remainder Theorem

THEOREM (Chinese Remainder Theorem)

Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime integers.

Let $a_1, a_2, \ldots, a_k$ be arbitrary integers. The system

$$\begin{cases} x \equiv a_1 [m_1] \\ x \equiv a_2 [m_2] \\ \cdots \\ x \equiv a_k [m_k] \end{cases}$$

has a solution c. Further, all the solutions are $c + \ell(m_1 \cdots m_k)$, $\ell \in \mathbb{Z}$.

The Chinese Remainder Theorem

$$\begin{cases} x \equiv a_1 [m_1] \\ x \equiv a_2 [m_2] \\ \dots \\ x \equiv a_k [m_k] \end{cases}$$

Proof .

EXISTENCE

The Chinese Remainder Theorem

UNIQUENESS

The Chinese Remainder Theorem

2 equations: METHOD “BY HANDS”

EXAMPLE

$$\textbf{Solve} \begin{cases} x \equiv 3[11] \, (1) \\ x \equiv 2[7] \quad (2) \end{cases}$$

The Chinese Remainder Theorem

2 equations: CONSTRUCTIVE METHOD

$$\begin{cases} x \equiv a_1 [m_1] \\ x \equiv a_2 [m_2] \end{cases}$$

The Chinese Remainder Theorem

2 equations: CONSTRUCTIVE METHOD

EXAMPLE Solve $\begin{cases} x \equiv 3[11] \\ x \equiv 2[7] \end{cases}$

$$\begin{aligned} m_1 u + \boxed{m_2 v} &= 1 \quad \times a_1 \\ m_2 v + \boxed{m_1 u} &= 1 \quad \times a_2 \end{aligned}$$

We use the constructive method of the proof.

The Chinese Remainder Theorem

3 equations: METHOD “BY HANDS”

EXERCISE
(Sun Tze Suan Ching)

$$\textbf{Find } x \in \mathbb{Z}\textbf{:} \begin{cases} x \equiv 2[3] \quad (1) \\ x \equiv 3[5] \quad (2) \\ x \equiv 2[7] \quad (3) \end{cases}$$

The Chinese Remainder Theorem

3 equations: CONSTRUCTIVE METHOD

EXAMPLE

$$\text{Solve} \begin{cases} x \equiv 2[3] \\ x \equiv 3[7] \\ x \equiv 4[16] \end{cases}$$

Use the constructive method of the proof.

$$m_1 = 3, m_2 = 7, m_3 = 16$$

Set $n_i := m_1 \cdots \widehat{m_i} \cdots m_k$.

For each $i = 1, \ldots, k$ we have $\gcd(m_i, n_i) = 1$:

Let $u_i, v_i \in \mathbb{Z} : \; m_i u_i + n_i v_i = 1$. coprimality

Define $x = \sum_{j=1}^{k} n_j v_j a_j$

The Chinese Remainder Theorem

EXAMPLE

$$\text{Solve} \begin{cases} x \equiv 2[3] \\ x \equiv 3[7] \\ x \equiv 4[16] \end{cases}$$

Use the constructive method of the proof.

$$m_1 = 3, m_2 = 7, m_3 = 16$$

The Chinese Remainder Theorem

EXAMPLE

The people in a town are lining up for a parade.

- When they line up 3 to a row, 1 person is left over.
- When they line up 5 to a row, 2 people are left over.
- When they line up 13 to a row, 1 is left over.

What is the smallest possible population of the town?

$$\text{Solve } \min x > 0 : \begin{cases} x \equiv 1[3] \\ x \equiv 2[5] \\ x \equiv 1[13] \end{cases}$$

Solution: $x = 157$

The Chinese Remainder Theorem

HOW ABOUT IF the integers are not coprime

$$\textbf{Does} \begin{cases} x \equiv 0[4] \\ x \equiv 1[6] \end{cases} \textbf{have solutions?}$$

NO: $x \equiv 0[4] \Rightarrow x$ **even.**

$x \equiv 1[6] \Rightarrow x$ **odd.**

UNIT 5
Euler's phi function

Euler's function phi

Leonhard Euler

1707-1783

DEFINITION (Euler's function phi, Euler's totient function)

Let $m \in \mathbb{N}_{\geq 1}$. The number of elements of $(\mathbb{Z}/m\mathbb{Z})^*$ is denoted by $\phi(m)$.

$$\phi(m) = \#\{1 \leq a \leq m : \gcd(a, m) = 1\}$$

This is why we require $a \leq m$ instead of $a < m$, as in [HPS].

EXAMPLE $\phi(1) = 1$

$\phi(14) = 6$

$m \geq 2 \Rightarrow m \notin \{1 \leq a \leq m : \gcd(a, m) = 1\} : \varphi(m) \leq m - 1$

REMARK $m \geq 2$ is prime $\Leftrightarrow \varphi(m) = m - 1$.

Compute Euler's function phi

THE CASE OF A POWER OF A PRIME

PROPOSITION **Let p be prime and $\alpha \geq 1$. Then $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.**

Proof.

A formula for computing Euler phi

THE GENERAL CASE

THEOREM Let $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ with p_i primes and $\alpha_i \geq 1$.

$$\text{Then } \phi(n) = \phi(p_1^{\alpha_1}) \cdots \phi(p_m^{\alpha_m}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_m^{\alpha_m} - p_m^{\alpha_m - 1})$$

$$= p_1^{\alpha_1} \cdots p_m^{\alpha_m} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

EXAMPLE $\phi(5^4 \cdot 7^3) = ?$

$\phi(3456) = ?$

A formula for computing Euler phi

FIRT PROOF (m=2)

THEOREM Let $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ with p_i primes and $\alpha_i \geq 1$.

Then $\phi(n) = \phi(p_1^{\alpha_1}) \cdots \phi(p_m^{\alpha_m}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_m^{\alpha_m} - p_m^{\alpha_m - 1})$

$$= p_1^{\alpha_1} \cdots p_m^{\alpha_m} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

First proof (Combinatorial approach).

A formula for computing Euler phi

SECOND PROOF (m=2)

THEOREM Let $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ with p_i primes and $\alpha_i \geq 1$.

Then $\phi(n) = \phi(p_1^{\alpha_1}) \cdots \phi(p_m^{\alpha_m}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_m^{\alpha_m} - p_m^{\alpha_m - 1})$

$$= p_1^{\alpha_1} \cdots p_m^{\alpha_m} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

Second proof. $\phi(p^a q^b) = \phi(p^a)\phi(q^b)$ **motivation?**

$$= (p^a - p^{a-1})(q^b - q^{b-1}). \quad \square$$

QUESTION **Is it true that $\phi(mn) = \phi(m)\phi(n)$?**

THEOREM (Multiplicative property of the Euler phi function)

The proof of the Theorem is based on the remainder map…

The remainder map

DEFINITION **Let $m, n \in \mathbb{N}$ be integers.**

The remainder map $r : \mathbb{Z}/(mn)\mathbb{Z} \longrightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ is

$$\forall a \in \{0, \ldots, mn-1\}\colon r((a)_{mn}) := ((a)_m, (a)_n).$$

EXAMPLE $m = 4, n = 9,\ r((11)_{36}) = \ ((11)_4, (11)_9) = ((3)_4, (2)_9)$

PROPOSITION **r is well defined:** $(a)_{mn} = (b)_{mn} \Rightarrow ((a)_m, (a)_n)) = ((b)_m, (b)_n))$.

Proof.

The remainder map

Is r one-to-one?

EXAMPLE (the case where m, n are not coprime)

Let $r : \mathbb{Z}/(4 \cdot 6)\mathbb{Z} \longrightarrow (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$,

$\forall a \in \{0, \ldots, 23\}$ $\qquad r((a)_{24}) := ((a)_4, (a)_6)$.

1) Is r injective?

2) Is r surjective?

Bijectivity of the remainder map for pairwise coprime integers

THEOREM (Bijectivity of the remainder map with coprime factors)

Let $m, n \in \mathbb{N}_{\geq 1}$ be pairwise coprime naturals.

The remainder map $r : \mathbb{Z}/(mn)\mathbb{Z} \longrightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ is one-to-one.

Proof.

SURJECTIVITY

INJECTIVITY

□

The remainder map for pairwise coprime integers

UNITS ARE SENT TO UNITS

PROPOSITION (Units are sent to units) **Let $m, n \in \mathbb{N}_{\geq 1}$ be naturals.**

Then $r\left((\mathbb{Z}/(mn)\mathbb{Z})^*\right) = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$.

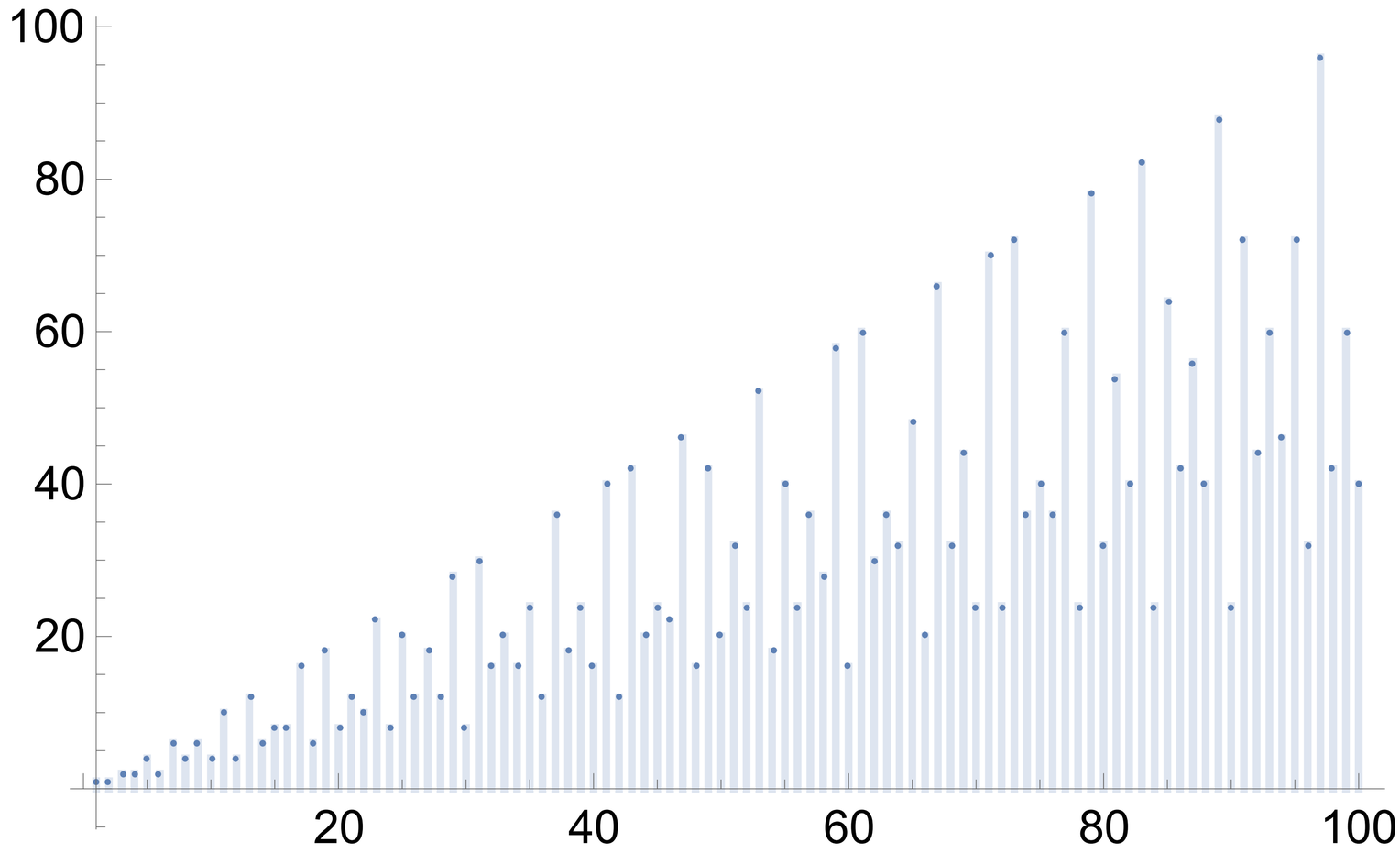
Proof.

COROLLARY (Multiplicativity of phi) **Let $m, n \in \mathbb{N}$ be pairwise coprime integers. Then $\phi(mn) = \phi(m)\phi(n)$.**

Proof.

Compute Euler's function phi

```
In[170]:= EulerPhi[180]
Out[170]= 48
```



Compute Euler's function phi

END of Lesson 3
Introduction to modular algebra