Euler Phi Function

Monday, February 7, 2022 12:40 PM

Missing #1, 2, 5, 6, 13, 32, 34

Recall: $a^{-1} \pmod m$

e.g. $14^{-1} \equiv 14 \pmod{15}$

1] Notations:

$\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ positive integers

$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

2] Exer: Find the inverse x^{-1} for all

① $x \in \mathbb{Z}_7$

x	0	1	2	3	4	5	6
x^{-1}	—	1	4	5	2	3	6

② $x \in \mathbb{Z}_{15}$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x^{-1}	—	1	8	—	4	—	—	13	2	—	—	11	—	7	14

3] Notation:

$\mathbb{Z}_n^* = \{x \mid x \in \mathbb{Z}_n \text{ and } \gcd(x, n) = 1\}$

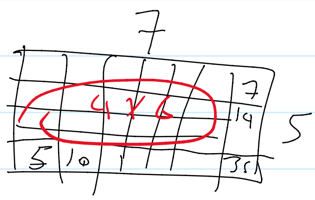
4] Def^n. (The Euler Phi function)

for $n \geq 1$, $\phi(n) = |\mathbb{Z}_n^*|$

e.g. $\phi(15) = 8$

$\phi(17) = 16$

$\phi(35) = 4 \cdot 6 = 24$



$\phi(105) = 2 \times 4 \times 6$

$105 = 3 \times 5 \times 7$

$\phi(3) = |\{1, 2\}| = 2$

$\phi(2) = |\{1\}| = 1$

$\phi(1) = |\{0\}| = 1$

$1 \in \mathbb{Z}_2 = \{0, 1\}$

$\gcd(1, 2) = 1$

$\gcd(0, 2) = 2 \neq 1$

$\mathbb{Z}_1 = \{0\}$ $\gcd(0, 1) = 1$

$\gcd(0,2) = 2 \neq 1$

$\mathbb{Z}_1 = \{0\}$ $\gcd(0,1) = 1$

$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$

$\phi(3^2) = 2 \cdot 3^1$

5] Algorithm: Compute $\phi(n)$

Thm: 1. $\phi(1) = 1$

2. $\phi(p^k) = (p-1) \cdot p^{k-1}$ for prime p

3. $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$ if $\gcd(m,n) = 1$

eg. $\phi(105) = \phi(21) \cdot \phi(5)$

$= \phi(3) \cdot \phi(7) \cdot \phi(5)$

$= 2 \cdot 6 \cdot 4 = 48$

$\phi(100) = \phi(10^2) = 9(10^1)$ ✗ 10 is not prime

$= \phi(2^2 \cdot 5^2) = \phi(2^2) \cdot \phi(5^2)$

$= (1 \cdot 2^1)\ (4 \cdot 5^1)$

$= 2 \cdot 20$

$= 40$

$\phi(14) = \phi(2) \cdot \phi(7)$

$= 1 \cdot 6 = 6$

$\phi(108) = \phi(2^2 \cdot 3^3)$

$= (1 \cdot 2^1)(2 \cdot 3^2)$

$= 2 \cdot 18$

$= 36$

6] Exer: Solve

$4x + 2y \equiv 7 \pmod{11}$ —— ①

$x - y \equiv 3 \pmod{11}$ —— ②

by ① + 2② $\Rightarrow 6x + 0y \equiv 13 \equiv 2 \pmod{11}$

$\Rightarrow x \equiv 2 \cdot 6^{-1}$

$\equiv 2 \cdot 2 \equiv 4 \pmod{11}$

$\therefore \boxed{x \equiv 4} \pmod{11}$

in ② $4 - y \equiv 3 \pmod{11}$

$y \equiv 1 \pmod{11}$

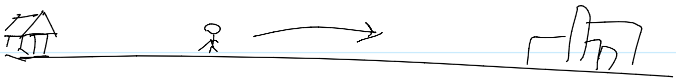
7] The Chinenese Remainder Theorem (CRT)

OBJECTIVE : ⊙ To solve a system of linear congruences

⊙ To perform arithmetic with large integers

Sun Tsu

$x \equiv 1 \pmod{2}$



$x \equiv 1 \pmod{3}$

$x \equiv 1 \pmod{4}$ $\qquad 2 \cdot 3 \cdot 4 \cdot 5 + 1 = 121$

$x \equiv 1 \pmod{5}$

8] Thrm : Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime integers. Then the system:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$

9] Proof : How to find the solution in the CRT

1. Let $M_k = m / m_k \Rightarrow \gcd(m_k, M_k) = 1$
2. Find $y_k = M^k \pmod{m_k} \Longrightarrow M_k \cdot y_k \equiv 1 \pmod{m_k}$

3. Then $x \equiv a_1 M_1 \cdot y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n \pmod{m}$

e.g.