

Chinese Remainder Theorem

$$\left. \begin{array}{l} x \equiv a_1 (m_1) \\ \vdots \\ x \equiv a_r (m_r) \end{array} \right\} (x) \quad \text{If } (m_i, m_j) = 1, \forall i \neq j, \text{ then a solution exists.}$$

In fact we find all solutions as follows:

$$m = m_1 \cdots m_r$$

$$\left(\frac{m}{m_i}, m_j \right) = \begin{cases} m_j & j \neq i \\ 1 & j = i \end{cases}$$

Let b_i be s.t. $b_i \left(\frac{m}{m_i} \right) \equiv 1 (m_i)$

$$x_0 = \sum_{i=1}^r b_i \left(\frac{m}{m_i} \right) a_i. \quad \text{All sol'n are } x_0 + ml, \quad l \in \mathbb{Z}$$

ex: Do $5x \equiv 1 (6)$ and $4x \equiv 13 (15)$ have a common solution?

$$5x \equiv 1 (6) \Leftrightarrow x \equiv 5 (6) \Leftrightarrow x \equiv 1 (2), x \equiv 2 (3)$$

$$4x \equiv 13 (15) \Leftrightarrow x \equiv 52 (15) \Leftrightarrow x \equiv 7 (15) \Leftrightarrow x \equiv 1 (3), x \equiv 2 (5)$$

no solution.

ex: Do $x \equiv 6 (15)$, $x \equiv 1 (20)$ have a common solution?

$$x \equiv 6 (15) \Leftrightarrow x \equiv 0 (3), x \equiv 1 (5)$$

$$x \equiv 1 (20) \Leftrightarrow x \equiv 1 (5), x \equiv 1 (4).$$

solution exists.

$$m = 3 \cdot 4 \cdot 5 = 60.$$

$$\frac{m}{m_1} = 20, \quad \frac{m}{m_2} = 15, \quad \frac{m}{m_3} = 12$$

$$b_1 = 2, \quad b_2 = 3, \quad b_3 = 3.$$

$$x_0 = 20(2) \cdot 0 + 15(3)(1) + 12(3) \cdot 1 = 45 + 36 = 81$$

$$\text{All solutions} = 81 + 60k$$

Theorem If $(m_1, m_2) = 1$, $m_1, m_2 > 0$.

Then $\phi(m_1 \cdot m_2) = \phi(m_1) \phi(m_2)$ In fact, if $m = \prod p_i^{\alpha_i}$, then

$$\phi(m) = \prod_p (p^{\alpha_i} - p^{\alpha_i - 1})$$

Proof:

$$\phi(m_1 \cdot m_2) = \# \{ n \mid 1 \leq n \leq m_1 \cdot m_2 \text{ and } (n, m_1 \cdot m_2) = 1 \} \quad \text{Set } S$$

$$\phi(m_1) \cdot \phi(m_2) = \# \{ (n_1, n_2) \mid 1 \leq n_1 \leq m_1, 1 \leq n_2 \leq m_2, (n_1, m_1) = 1, (n_2, m_2) = 1 \} \quad \text{Set } S_2$$

Define map $\Gamma: S_2 \rightarrow S$. $\Gamma(n) = (n_1, n_2)$ where $1 \leq n_i \leq m_i$ and $n_i \equiv n (m_i)$

Note: $(n, m_1 \cdot m_2) = 1 \Rightarrow (n, m_i) = 1$, so $(n_1, n_2) \in S_2$

Γ bijective.

Given $(n_1, n_2) \in S_2$, $\exists!$ $n \in S$ s.t. $\Gamma(n) = (n_1, n_2)$.

The equations $x \equiv n_1 (m_1)$ $x \equiv n_2 (m_2)$ have a solution n by Chinese Remainder Thm, and n is unique up to adding $l(m_1 \cdot m_2)$.

Thus, there is a unique solution in interval $1 \leq n \leq m_1 \cdot m_2$.

Show $(n, m_1 \cdot m_2) = 1$. If pln , $plm_1 \cdot m_2$, then pln and plm_1 or plm_2

Either $(n, m_1) \neq 1$ or $(n, m_2) \neq 1$, contradiction.

Note: Part 1 of Thm implies that to prove 2nd statement it is enough to consider $m = p^\alpha$

compute $\phi(p^\alpha) = \{1, 2, \dots, p^\alpha\}$

$$p^\alpha - \#\{n \mid 1 \leq n \leq p^\alpha, p|n\} = p^\alpha - \#\{ph \mid 1 \leq h \leq p^{\alpha-1}\} = p^\alpha - p^{\alpha-1}$$

Def. Fix polynomial $f(x)$. For integer m , write

$$N_f(m) = \# \text{ of sol'n of } f(x) \equiv 0 \pmod{m}$$

i.e. # of elts. in $\{1, \dots, m\}$ for which congruence holds.

Thm: If $(m_1, m_2) = 1$, then $N_f(m_1 m_2) = N_f(m_1) N_f(m_2)$.

Proof:

$$\{n \mid 1 \leq n \leq m_1 m_2, f(n) \equiv 0 \pmod{m_1 m_2}\} = S,$$

$$\{(n_1, n_2) \mid 1 \leq n_i \leq m_i, f(n_i) \equiv 0 \pmod{m_i}, i=1, 2\}.$$

Again, define $\Gamma: S \rightarrow S_2$ $n \mapsto (n_1, n_2)$ with $n_i \equiv n \pmod{m_i}$.

(CRT \Rightarrow given $(n_1, n_2) \exists!$ n $1 \leq n \leq m_1 m_2$ with $\Gamma(n) = (n_1, n_2)$.)

check: $f(n) \equiv 0 \pmod{m_1 m_2} \Leftrightarrow f(n_1) \equiv 0 \pmod{m_1} \wedge f(n_2) \equiv 0 \pmod{m_2}$.

$\Leftrightarrow f(n) \equiv 0 \pmod{m_1}, f(n) \equiv 0 \pmod{m_2}$, which is true