CS 70 Discussion 4A

September 25, 2024

Extended Euclid's Algorithm

Finds values $x, y \in \mathbb{Z}$ for some given $a, b \in \mathbb{N}$ such that:

$$ax + by = \gcd(a, b)$$

The efficient algorithm is as follows (return value is of form $(x, y, \gcd(a, b))$):

function $\textsc{E\_GCD}(a,\ b)$
  if $b = 0$ **then return** $(1, 0, a)$
  else
    $(x, y, z) \leftarrow \textsc{E\_GCD}(b, a \bmod b)$
    return $(y, x - \lfloor \frac{a}{b} \rfloor y, z)$
  end if
end function

You can use EGCD to get inverses iff (if and only if) $\gcd(a, b) = 1$:

$$a^{-1} \equiv x \pmod{b}$$
$$b^{-1} \equiv y \pmod{a}$$

Fermat's Little Theorem

Following is true for any prime p and $a \not\equiv 0 \pmod{p}$:

$$a^{p-1} \equiv 1 \pmod{p}$$

The following general variant is true for any prime p and *any* $a \in \mathbb{Z}$:

$$a^p \equiv a \pmod{p}$$

Chinese Remainder Theorem

Problem Setup: You're given variables $m_1, m_2, ..., m_n \in \mathbb{N}^+$ and $a_1, a_2, ..., a_n \in \mathbb{Z}$ where $(\forall i \neq j)(\gcd(m_i, m_j) = 1)$ (the set of m_i's is pairwise *coprime*). We want to find a $x \in \mathbb{Z}$ where:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

Conclusion: There always exists a *unique* solution $x \pmod{M}$ where $M = \prod_{i=1}^{n} m_i$.

Chinese Remainder Theorem (Cont.)

Solution: For the system $(\forall i \in \{1, 2, ..., n\})(x \equiv a_i \pmod{m_i})$ where $(\forall i \neq j)(\gcd(m_i, m_j) = 1)$:

$$x \equiv \sum_{i=1}^{n} a_i b_i \pmod{M}$$

$$b_i = \frac{M}{m_i}\left[\left(\frac{M}{m_i}\right)^{-1} \pmod{m_i}\right]$$

$$M = \prod_{i=1}^{n} m_i$$