Discrete Mathematics

Number Theory and Cryptography

Prof. Steven Evans

4.4: Solving Congruences

Solving congruences

Theorem

If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Further, this inverse is unique modulo m. (That is, there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.)

The Chinese Remainder Theorem

Theorem

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

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

has a unique solution modulo $m = m_1 \cdots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

The Chinese Remainder Theorem

Proof of existence

To construct a simultaneous solution, first let $M_k = m/m_k$ for $k = 1, 2, \ldots, n$. That is, M_k is the product of the moduli except for m_k. Because m_i and m_k have no common factors greater than 1 when $i \neq k$, it follows that $\gcd(m_k, M_k) = 1$. Consequently, we know there is an integer y_k, an inverse of M_k modulo m_k, such that $M_k y_k \equiv 1 \pmod{m_k}$.

The Chinese Remainder Theorem

Proof of existence

To construct a simultaneous solution, first let $M_k = m/m_k$ for $k = 1, 2, \ldots, n$. That is, M_k is the product of the moduli except for m_k. Because m_i and m_k have no common factors greater than 1 when $i \neq k$, it follows that $\gcd(m_k, M_k) = 1$. Consequently, we know there is an integer y_k, an inverse of M_k modulo m_k, such that $M_k y_k \equiv 1 \pmod{m_k}$.

To construct a simultaneous solution, form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n.$$

Note that $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$. Hence, only the kth term in this sum survives reduction modulo m_k. We then see

$$x \equiv a_k(M_k y_k) \equiv a_k \pmod{m_k}.$$

The Chinese Remainder Theorem

Example

Consider the system

$$x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 5, \qquad x \equiv 2 \mod 7.$$

We calculate the pieces we need for the proof stated above:

$$\begin{aligned} m &= 3 \cdot 5 \cdot 7 = 105, \\ M_1 &= m/3 = 35, & y_1 &\equiv M_1^{-1} \equiv 2 \pmod 3, \\ M_2 &= m/5 = 21, & y_2 &\equiv M_2^{-2} \equiv 1 \pmod 5, \\ M_3 &= m/7 = 15, & y_3 &\equiv M_3^{-1} \equiv 1 \pmod 7. \end{aligned}$$

Then:

$$\begin{aligned} x &\equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}. \end{aligned}$$

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

If p is prime and a is an integer not divisible by p, then

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

Further, for every integer a we have

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

Fermat's Little Theorem

Example

Find $7^{222} \pmod{11}$.

Fermat's Little Theorem

Example

Find $7^{222} \pmod{11}$.

By Fermat's little theorem, we know that $7^{10} \equiv 1 \pmod{11}$, so $(7^{10})^k \equiv 1 \pmod{11}$ for every positive integer k. Division yields $22 = 22 \cdot 10 + 2$, and hence

$$7^{222} = 7^{22 \cdot 10+2} = (7^{10})^{22} \cdot 7^2 \equiv 1^{22} \cdot 49 \equiv 5 \pmod{11}.$$