Fermat's and Euler's Theorem:

Two theorems that play important roles in public-key cryptography are Fermat's and Euler's theorem.

Fermat's theorem:

Fermat's theorem states that: If p is prime and a is a positive integer not divisible by p, then:

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

Proof: Consider the set of positive integers less than k: $\{1, 2, 3 \ldots k-1\}$ and multiply each element by a, modulo k to get,

$$\text{Set } X = \{a \bmod p,\ 2a \bmod p, \ldots (p-1)a \bmod p\}$$

Since p does not divide, no element in X is 0. Furthermore, no two integers in X are equal. Since, assume that $ja == ka \pmod{p}$ where $1 <= j < k <= p-1$. Because a is relatively prime* to p, we can eliminate a from both sides,

$$j == k \pmod{k}$$

Since j and k are both less than k, this equality is impossible.

$\therefore$ all $(p-1)$ elements in set X are unequal.

Hence, we can conclude X consists of set of integers: {1, 2, 3 ... ~~1~~ p−1} in some order.

Multiplying the numbers in both sets (p and x) and taking the result mod p yields.

$$a \times 2a \times \ldots (p-1)a \equiv [(1 \times 2 \times \ldots (p-1)] (\text{mode } p)$$

$$a^{p-1}(p-1)! \equiv (p-1)! (\text{mod } p).$$

Example:

Let p = 17, an integers prime number.
a = 2, an integer not a multiple of p.

According to Fermat's little theorem:

$2^{17-1} \equiv 1 \bmod 17$.

we got $65536 \,\%\, 17 \equiv 1$.

that mean $(65536 - 1)$ is a multiple of 17.

Euler's theorem:

This theorem states that for every a and n that are relatively prime.

$$a^{\phi(n)} \equiv 1 (\text{mod } n).$$

Proof: If n is prime, $\phi(n) = (n-1)$ and Fermat's theorem holds. However it holds for any integer n. As we know, $f(n)$ is the number of positive integers less than n, that are relatively prime to n.

Scanned by TapScanner

Consider the set of integer R,

$R = \{x_1, x_2 \dots , x_{\phi(n)}\}$.

Each element x_i is a unique positive integer less than n with GCD$(x_i, n) = 1$.

Multiply each element by a, modulo n.

$S = \{(ax_1 \bmod n), (ax_2 \bmod n) \dots (ax_{\phi(n)} \bmod n)\}$

The set S is a permutation of R because a is relatively prime to n and x is relatively prime to n. Thus all the members of S are integers that are less than n and that are relatively prime to n.

Since there are no duplicates in S, If $ax_i \bmod n = ax_j \bmod n$, then:

$$x_i = x_j.$$

$$\therefore \prod_{i=1}^{\phi(n)} (ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i.$$

$$\prod_{i=1}^{\phi(n)} ax_i = \prod_{i=1}^{\phi(n)} x_i \pmod n$$

$$a^{\phi(n)} \times \left[\prod_{i=1}^{\phi n} x_i\right] \equiv \prod_{i=1}^{\phi(n)} x_i \pmod n$$

$$a^{\phi(n)} \equiv 1 \pmod n$$

Example:

Euler's method can be used to take a time-based system of ODEs and transform it into a different equation using Euler's method so that we can use it in dynamic programming or discrete optimal control approaches.

2. Chinese remainder theorem :

The chinese remainder theorem is a theorem which gives a unique solution to simultaneous linear congruences with coprime moduli. In its basic form, the Chinese remainder theorem will determine a number p that, when divided by some given divisors, leaves given remainders.

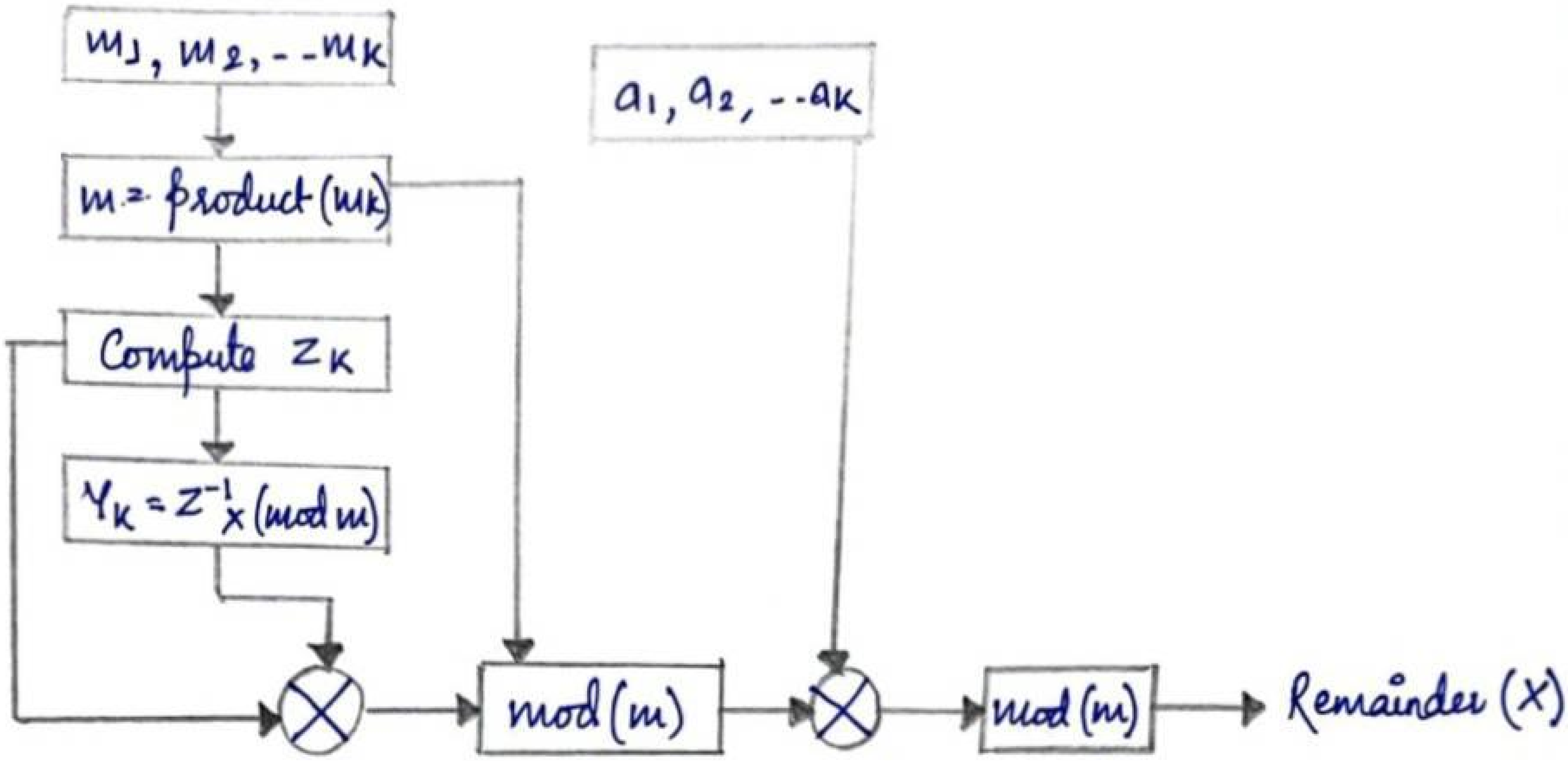
Given pairwise coprime positive integers $n_1, n_2, \ldots, n_k$ and arbitary integers $a_1, a_2, \ldots, a_k$, the system of simultaneous congruences:

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_k \pmod{n_k}$$

has a solution, and the solution is unique modulo $N = n_1 n_2 \ldots n_k$.

Solution → Find $M = m_1 \times m_2 \times \ldots m_k$.
Find $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2} \ldots M_k = \frac{M}{M_k}$.

Find multiplicative inverse of $M_1, M_2, \ldots M_k$ i.e, M_1^{-1}, $M_2^{-1} \ldots M_k^{-1}$.
Solution is calculated as:
$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \ldots + a_k \times M_k \times M_k^{-1})$ mod M.



Example:

$x \equiv 6 \pmod{11}$, $x \equiv 13 \pmod{16}$, $x \equiv 9 \pmod{21}$, $x \equiv 19 \pmod{25}$

$M_1 = \frac{M}{M_1} = 16 \times 21 \times 25 = 8400$, $M_2 = 11 \times 21 \times 25 = 5775$.

$M_3 = 11 \times 16 \times 25 = 4400$, $M_4 = 11 \times 16 \times 21 = 3696$.

$M_1^{-1} = 8400^{-1} \pmod{m_1} = 8400^{-1} \pmod{11} = 4^{-1} \pmod{11} = 8 \pmod{11}$

$M_2^{-1} = 5775^{-1} \pmod{16} = 15 \pmod{16}$

$M_3^{-1} = 4400^{-1} \pmod{21} = 2 \pmod{21}$

$M_4^{-1} = 3696^{-1} \pmod{25} = 6 \pmod{25}$

$x = 6 \times 8 \times 8400 + 13 \times 15 \times 5775 + 19 \times 6 \times 3696 + 9 \times 2 \times 4400$.

$x = 51669 \bmod m = 51669 \bmod (m_1 m_2 m_3 m_4)$

$x = 51669 \pmod{92400}$.

Real world example:

Used to solve multiple range ambiguities in many radar systems.

Advantages:

It is useful for discerning solutions to congruence problems which are used in cryptographic algorithms like RSA as well as factorization.

Disadvantages:

It can't be used if moduli are not co-prime as multiplicative inverse cannot be found.

Indu Singh, AP, CSE, DTU