CIS 5371 Cryptography

6. An Introduction to Number Theory

Congruence and Residue classes

- Arithmetic modulo n, Z_n
- Solving linear equations
- The Chinese Remainder Theorem
- Euler's phi function
- The theorems of Fermat and Euler
- Quadratic residues
- Legendre & Jacobi symbols

Arithmetic modulo n

Examples

- $Z_n = \{0,1,2, \ldots , n\text{-}1\}$,
- $Z_p^* = \{1,2, \ldots , p\text{-}1\}$, for prime p,
- $Z_n^* = \{$all integers k, $0 < k < n$, with $gcd(k,n) = 1\}$.

Solving linear equations

Theorem

For any integer $n > 1$,

$$ax \equiv b \pmod{n}$$

is solvable, if and only if, $\gcd(a,n) \mid b$.

Examples

$6x \equiv 18 \pmod{36}$ has 6 solutions: 3, 9, 15, 21, 27, 33.

$2x \equiv 5 \pmod{10}$, has no solutions.

The Chinese Remainder Theorem

Let $m_1, \ldots, m_n$ be positive integers with $\gcd(m_i, m_j) = 1$,

and let $M = m_1 m_2 \cdots m_r$.

Then the congruence

$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$
$$\vdots \quad \vdots \qquad \vdots$$
$$x \equiv c_r \pmod{m_r}$$

has a *unique* solution $z \in Z_M$.

The Chinese Remainder Theorem

Let $(M/m_i).y_i \equiv 1 \pmod{m_i}$. Then for

$$z_i = (M/m_i).y_i$$

it is easy to see that

$$z \leftarrow \sum_{i=1}^{r} z_i c_i \pmod{M}$$

is a solution.

Example

Solve the modular conguence :

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 4 \pmod 7$

We have : $M = 105$,

$y_1 \equiv 35^{-1} \pmod 3 \equiv 2 \pmod 3$

$y_2 \equiv 21^{-1} \pmod 5 \equiv 1 \pmod 5$

$y_3 \equiv 15^{-1} \pmod 7 \equiv 1 \pmod 7$

Then $z \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 4 \cdot 15 \cdot 1 \equiv 263 \bmod 105 \equiv 53 \bmod 105$

Example

Solve the modular conguence :

$$x \equiv 1 \pmod{2}$$

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{7}$$

Euler's phi function

$\phi(n)$ is the number of positive integers k for which $\gcd(k,n)=1$. We have

$\phi(1)=1$

$\phi(p)=p-1$, p a prime,

$\phi(pq)=(p\text{-}1)(q\text{-}1)$, for p,q primes,

$$\phi(p^e)=p^e-p^{e-1}=p^e(1-\frac{1}{p}),\ \ p \text{ a prime, e} > 1.$$

It follows that if $n = p_1^{e_1}\cdot p_1^{e_2}\cdot\cdots\cdot p_1^{e_1}$, is the prime factorization of n, then

$$\phi(n)=n\,(1-\frac{1}{p_1})\cdot(1-\frac{1}{p_2})\cdot\ldots\cdot(1-\frac{1}{p_k}).$$

The theorems of Fermat and Euler

Fermat's little theorem

If p is prime then,

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

for all integers a: 0 < a < p.

Euler's theorem

If $\gcd(a,n)=1$ *then* $a^{\varphi(n)} \equiv 1 \pmod{n}$,

Legendre & Jacobi symbols

Let QR_p be the set of quadratic residues mod p and let

$QNR_p = Z_p^* \setminus QR_p$ be the set of quadratic nonresidues.

For $x \in Z_p^*$, p prime, the *Legendre* symbol of x mod p is:

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & if \;\; x \in QR_p^{p^e} \\ -1 & if \;\; x \in QNR_p \end{cases}$$

Let $n = p_1 p_2 \cdots p_k$ be the prime factorization of n.

For $x \in Z_n^*$, the *Jakobi* symbol of n mod p is:

$$\left(\frac{x}{n}\right) = \left(\frac{x}{p_1}\right)\left(\frac{x}{p_2}\right)\cdots\left(\frac{x}{p_k}\right)$$

Legendre & Jacobi symbols

It is easy to see that

$$\left(\frac{x}{p}\right) = x^{(p-1)/2} \pmod{p}, \text{ for } p \text{ prime.}$$

Legendre & Jacobi symbols

We have :

$$\left(\frac{1}{n}\right) = 1, \text{ and } \left(\frac{xy}{n}\right) = \left(\frac{x}{n}\right)\cdot\left(\frac{y}{n}\right)$$

$$\left(\frac{x}{mn}\right) = \left(\frac{x}{m}\right)\cdot\left(\frac{x}{n}\right)$$

If $x \equiv y \pmod{n}$ then $\left(\frac{x}{n}\right) = \left(\frac{y}{n}\right)$

For m, n odd :

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$$

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$$

If $\gcd(m,n) = 1$ and $m, n > 2$ then $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4}$

Example

Compute $\left(\frac{4}{15}\right)$ and $\left(\frac{7}{15}\right)$