Lecture 16: Properties of Modular Congruence, Euler's Totient Function, RSA

Summary:
We explore properties of modular arithmetic and their applications to cryptography. We prove Fermat's little theorem and examine Euler's totient function, establishing its properties for semiprime numbers. We conclude with an introduction to RSA encryption, demonstrating how these concepts enable secure communication.

Topics Covered: Euler totient function, Euler totient theorem, Fermat's little theorem, modular congruence, semiprime, RSA

Proposition 1:

Let $a \in \mathbb{Z}$ and let p be prime. Then,

1. $a^p \equiv a \pmod{p}$
2. $a^{k(p-1)+1} \equiv a (\bmod p),\ k \in \mathbb{Z}_{\geq 0}$

Example:

Let

$$p(x) = 2x^7 + x^5 + 3x^3 + 4x + 10$$

Prove that $p(n) \equiv 0 \ (\bmod 5)$

Proof:

We know that for any prime p, in particular, for $p = 5$, that

$$\forall a \in \mathbb{Z},\ a^p = a \ (\bmod p)$$

$$\implies \forall a \in \mathbb{Z}.\ a^5 = a \ (\bmod 5)$$

$$(2x^7 + x^5 + 3x^3 + 4x + 10) \equiv 2x^3 + x + 3x^3 + 4x + 10$$

$$\equiv 5x^3 + 5x + 10 = 5(x^3 + x + 2) \equiv 0 \bmod 5$$

$$\text{QED}$$

Definition:

A positive integer n is semiprime if $n = pq$ for distinct primes p, q.

For example,

$$\phi(n) = (p-1)(q-1) = pq - p - q + 1$$

There are a total of q multiples of $p \leq n$

There are a total of p multiples of $q \leq n$

Then, we have to add back 1, we overcounted one of the primes

For example, in the case of $n = 5 \cdot 3$, we overcounted 15.

The total number of numbers $\leq n$ that are not relatively prime ot n is $p + 1 - \text{however many are divisible}$

Proposition 2:

Let $a \in \mathbb{Z}$ and let $n = pq$ be semiprime,. Then,

$$a^{k\phi(n)+1} \equiv a \pmod n,\ \forall k \in \mathbb{Z}_{\geq 0}$$

Proof:

Proposition 1 part 2 says that for primes p and q, we have

$$a^{r(p-1)+1} \equiv a \pmod p,\ r \in \mathbb{Z}_{\geq 0}$$

$$a^{s(q-1)+1} \equiv a \pmod q,\ \forall s \in \mathbb{Z}_{\geq 0}$$

Set $r = k(q-1),\ k \in \mathbb{Z}_{\geq 0}$, $s = k(p-1),\ k \in \mathbb{Z}_{\geq 0}$

The lemma implies that

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

Lemma:

Let $a, b, r, s \in \mathbb{Z}$. Then,

- $a \equiv b \pmod r$
- $a \equiv b \pmod s$

  $\iff$

$$a \equiv b(\bmod(\operatorname{lcm}(r, s)))$$

$\impliedby$ **proof:**

$$a \equiv b \ (\bmod(\operatorname{lcm}(r, s))) \implies \text{lemma} \implies a \equiv b \pmod r \implies a \equiv b \pmod s$$

RSA encryption:

Let Alice pick a semiprime $n = pq$ where p and q are distinct primes.

Alice also picks an integer e such that $\gcd(e, \phi(n)) = 1$.

Alice finds d, the multiplicative inverse of $e \pmod{\phi(n)} = 1$

$$de \equiv 1 \pmod{\phi(n)}$$

$$de + k\phi(n) = 1$$

Alice makes n, e public, and she keeps p, q, d private

Alice picks

- $p = 47$
- $q = 59$
- $n = pq = 2773$

$$\phi(n) = (p-1)(q-1) = 2668$$

$e = 17$ such that $\gcd(e, \phi(n)) = 1$

Then, we use the extended Euclidean algorithm

$$157 \cdot 17 = (-1)(2668) = 1$$

$$d = 157$$

Message: THIS IS ALL GREEK TO ME

We encode the message as follows

- blank space = 00
- $A = 01$

- $B = 02$
- $....$
- $Z = 26$

Bob writes a message and turns it into an integer (or a sequence of integers) $0 \leq x \leq n$

Bob sends the residue $x^e \pmod{n}$ through the chanel

Alice gets $x^e \pmod{n}$ and computes

$$(x^e)^d \equiv x^{de} \equiv x^{-k\phi(n)+1} \equiv x \pmod{n}$$

Where the last equivalence follows from proposition 2.

Thus, Alice can recover x.

Proposition:

Let n be semiprime with $n = pq$ and p, q prime.

Then, p and q are uniquely determined by n and $\phi(n)$.

Proof:

Consider the equation

$$x^2 + (\phi(n) - n - 1)x + n = 0$$

$$x^2 + bx + c = 0$$

$$\implies (x - \alpha)(x - \beta)$$

Then, we have that

$$b = -(\alpha + \beta),\ c = \alpha\beta$$

$$\phi(b) = (p-1)(q-1) = pq - (p+1) + 1 \implies \phi(n) - n - 1 = -(p+q)$$

The solutions to this equation are exactly p and q

$$\text{QED}$$