

Cryptography and Data Security



Number Theory (2 of 2)

(presented by Aleksandr Yampolskiy)

Review

- Integers mod n : $Z_n = \{0, 1, \dots, n-1\}$
- Multiplicative integers mod n :
 $Z_n^* = \{x \in Z_n : \text{all } x \text{ relatively prime to } n\}$
- **Example:**
 - $Z_6 = \{0, 1, 2, 3, 4, 5\}$
 - $Z_6^* = \{1, 5\}$

Review (cont.)

- **Euler's totient function:** $\phi(n) = |\mathbb{Z}_n^*|$
 - $\phi(mn) = \phi(m)\phi(n)$
 - $\phi(p^k) = p^k - p^{k-1}$
- In general, $\phi(\prod_i p_i^{e_i}) = \prod_i (p_i^{e_i} - p_i^{e_i-1})$
- **Q:** How many integers in $[0, 12]$ are relatively prime to 12?
A: Four. They are $\{1, 5, 7, 11\}$.
$$\phi(12) = \phi(2^2 \cdot 3) = (2^2 - 2^1)(3^1 - 3^0) = 4.$$

Euler's Theorem

- **Recall:** if G is a finite group, $\forall x \in G, x^{|G|} = e$
- **Euler's Theorem:** $x^{\phi(n)} \equiv 1 \pmod{n}$, where $x \in \mathbb{Z}_n^*$.
Proof: Let $G = \mathbb{Z}_n^*$, which means $|G| = |\mathbb{Z}_n^*| = \phi(n)$. ?
- **Fermat's Theorem:** $x^{p-1} \equiv 1 \pmod{p}$, where $x \in \mathbb{Z}_p^*$ for some prime p .
Proof: Set $n = p$ and apply Euler's Theorem. ?

Euler's Theorem (cont.)

- **Example 1:**

- Let $p = 7$ so that $Z_p^* = \{1, 2, 3, 4, 5, 6\}$.
- Then, $2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1 \pmod{7}$

- **Example 2:**

- $x^a \equiv x^{a \bmod \phi(n)} \pmod{n}$, where $x \in Z_n^*$
- For RSA, $e \in Z_{\phi(n)}^*$ and $ed \equiv 1 \pmod{\phi(n)}$ so $(x^e)^d = x^{ed} = x^{ed \bmod \phi(n)} = x \pmod{n}$.

Greatest Common Divisor

- **Greatest Common Divisor** $\text{GCD}(a, b)$ is the largest number that divides both a and b
- $\text{GCD}(a, b) = \max \{k \in \mathbf{Z} : k|a \wedge k|b\}$
 - **Example:** $\text{GCD}(60, 24) = 12$
- If a and b share no common factors, they are called **relatively prime**.
 - **Example:** $\text{GCD}(7, 24) = 1$

Euclid's Algorithm

- GCD(a, b) can be computed using **Euclid's algorithm**
- Main idea: $\text{gcd}(a, b) = \text{gcd}(b, a \bmod b)$
- Let $a > b > 0$ and $\Phi = (1 + \sqrt{5})/2$. Then, algorithm terminates in at most $(\log b) / (\log \Phi) + 1$ iterations.
- **Example:**
 $\text{gcd}(55, 22) = \text{gcd}(22, 55 \bmod 22) = \text{gcd}(22, 11) = 11.$

Euclid's Algorithm

```
while (b != 0)
{
    r = a % b;
    a = b;
    b = r;
}
```

gcd(1970, 1066) = ?

$$1970 = 1 \times 1066 + 904$$

$$1066 = 1 \times 904 + 162$$

$$904 = 5 \times 162 + 94$$

$$162 = 1 \times 94 + 68$$

$$94 = 1 \times 68 + 26$$

$$68 = 2 \times 26 + 16$$

$$26 = 1 \times 16 + 10$$

$$16 = 1 \times 10 + 6$$

$$10 = 1 \times 6 + 4$$

$$6 = 1 \times 4 + 2$$

$$4 = 2 \times 2 + 0$$

gcd(1066, 904)

gcd(904, 162)

gcd(162, 94)

gcd(94, 68)

gcd(68, 26)

gcd(26, 16)

gcd(16, 10)

gcd(10, 6)

gcd(6, 4)

gcd(4, 2)

gcd(2, 0)

Euclid's Algorithm (cont.)

Thm: If $d = \gcd(a, b)$, then $\exists x, y \in \mathbb{Z}$ such that $ax + by = d$.

Thm: On input a, n such that $\gcd(a, n) = 1$, we can use Euclid's algorithm (extended) to compute b such that $ab \equiv 1 \pmod{n}$.

Finding Inverses

- Suppose $\gcd(a, b) = 1$. We can use extended Euclidean algorithm to find inverses.

$$\left\{ \begin{array}{l} a = q_1b + r_1 \\ b = q_2r_1 + r_2 \\ r_1 = q_3r_2 + r_3 \\ r_2 = q_4r_3 + r_4 \\ \dots \end{array} \right.$$

- In the first iteration we have a linear equation, so we can write: $r_1 = a - q_1b$
- In the second iteration, we similarly solve: $r_2 = b - q_2r_1 = b - q_2(a - q_1b) = (q_1q_2 + 1)b - q_2a$
- At each step we combine to get such an equation until we get $1 = a \cdot x + b \cdot y$ for some x, y
 - $a^{-1} = x \pmod b$
 - $b^{-1} = y \pmod a$

Polynomials over fields

- Let $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \dots + a_1 \cdot x + a_0$ be a polynomial of degree n in one variable x over a field F (namely, $a_n, a_{n-1}, \dots, a_0 \in F$).
- Polynomials over F , denoted as $F[x]$
- **Theorem:** The equation $f(x)=0$ has at most n solutions in F .
- However, the theorem does not hold over rings with identity.
 - E.g., in Z_{24} the equation $6 \cdot x = 0$ has six solutions $(0, 4, 8, 12, 16, 20)$.

[Polynomials over fields (cont.)]

- We'll be dealing with polynomials whose coefficients are in \mathbb{Z}_p (especially, $p = 2$).
- Consider, $f(x) = x^3 + x^2$ and $g(x) = x^2 + x + 1$ with coefficients in \mathbb{Z}_2 :
 - $f(x) + g(x) = x^3 + x + 1$
 - $f(x) \times g(x) = x^5 + x^2$

[Polynomials over fields (cont.)]

- Let $f(x) = \sum_{i=0}^n a_i x^i$ and $g(x) = \sum_{j=0}^m b_j x^j$ be two polynomials over F such that $m < n$.
- **Theorem:** There is a unique polynomial $r(x)$ of degree less than m over F such that $f(x) = h(x)g(x) + r(x)$.
- $r(x)$ is called the **remainder** of $f(x)$ modulo $g(x)$.
- if $f(x)$ has no divisors other than itself and 1 say it is **irreducible** (or prime) polynomial

Finite fields

- Finite fields play a key role in cryptography
- **Def:** A field $(F, +, \cdot)$ is **finite** if $|F| < \infty$.
- **Theorem** (Galois): For every prime power p^k ($k=1,2,\dots$) there is a **unique** finite field containing p^k elements. These fields are denoted by $GF(p^k)$. There are **no finite fields** with other cardinalities.

Finite fields (cont.)

- **Example:** To find a field of size 4, we try to find an irreducible polynomial of degree 2.
- $a^2 + a + 1 = 0$.
- **Note:** Our calculations are over \mathbb{Z}_2 so $a+b = a - b$.

GF(4) (·)	0	1	a	a ²
0	0	0	0	0
1	0	1	a	a ²
a	0	a	a²	1
a ²	0	a ²	1	a

GF(4) (+)	0	1	a	a ²
0	0	1	a	a ²
1	1	0	a ²	a
a	a	a ²	0	1
a ²	a ²	a	1	0