Information Systems Security (SOEN321)

A Brief introduction to number Theory

Dr. Amr Youssef

Concordia Institute for Information Systems Engineering (CIISE)
Concordia University
Montreal, Canada

youssef@ciise.concordia.ca

Why do we need to learn number theory

- Many public key systems are based on number theoretic ideas
- Examples include
  - RSA (based on the difficulty of factoring)
  - Diffie-Hellman (based on the difficulty of solving the discrete log problem)
  - El-Gamal (based on discrete log)
  - etc.
- We will no dive deep into number theory. We will only learn what is necessary to understand these systems

Modular Arithmetic

- **Definition:**

  a mod n = r $\Leftrightarrow \exists$ q s.t. a=q x n + r, where $0 \le r \le n-1$

- **Example:**
  - 7 mod 3 = 1
  - -7 mod 3 = 2

- **Definition (Congruence)**

$$a \equiv b \bmod n \Leftrightarrow a \bmod n = b \bmod n$$

Groups

- **Definition:**

A group $(G, *)$ is a set G on which a binary operation $*$ is defined which satisfies the following axioms:

- Closure: For all $a, b \in G$, $a * b \in G$
- Associative: For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$
- Identity: $\exists\ e \in G$ s.t. for all $a \in G$, $a * e = a = e * a$
- Inverse: For all $a \in G$, $\exists\ a^{-1} \in G$ s. t. $a * a^{-1} = a^{-1} * a = e$

Example

- $(Z_n, +)$, where
  - $Z_n = \{0, 1, \ldots, n - 1\}$,
  - a **+** b = a + b mod n
- $(Z_p^*, \times)$, where
  - $Z_p^* = \{1, \ldots, p - 1\}$
  - a **×** b = a × b mod p
- Abelian Group
  - A group $(G, *)$ is called an abelian group if * is a commutative operation:
  - Commutative: For all $a, b \in G$, $a * b = b * a$.

More explicit

- Example: $(Z_7, +)$
  - elements: {0,1,2,3,4,5,6}
  - 5+4=2
  - 0 is identity element
  - every element x has an inverse y such that $x+y=0$, what is the inverse of 3?
    - 3+4=0, thus the inverse of 3 is 4.
- Example: $(Z_7, \times)$
  - elements: (1,2,3,4,5,6)
  - what is the identity element?
  - what is the inverse of 3?
    - $3\times1=3$, $3\times2=6$, $3\times3=2$, $3\times4=5$, $3\times5=1$, $3\times6=4$

Fields

- a fields F is a commutative ring in which all non-zero elements have multiplicative inverses
- Finite fields: if F contains a finite number of elements
  - the order must be of type p^m with m>=1
  - for every order p^m there is a unique (up to isomorphism) $GF(p^m)$
- Example:The field: $Fp=(Z_p,+, \times)$
- Example: F_7
  - solve $3x+1=6$
  - $3x = 5$
  - $x = 3^{-1}\times5 = 5\times5=4$

Useful tools

- Extended Euclidian Algorithm
- Euclid's Theorem
- Chinese reminder theorem

Euclidian Algorithm

```
gcd (b, a)
        d=a;  t=b
        while t ≠0 {
                w ← d mod t
                d ← t
                t ← w
        }
        return d
```

Towards Extended Euclidian Algorithm

- **Theorem:** Given integers a, b > 0 and a > b, then d = gcd(a,b) is the least positive integer that can be represented as ax + by, x, y integer numbers.
- Corollary: if a and b are relative prime, then there exist x and y such that ax + by = 1.
- In other words, ax mod b = 1.
- How to find such x and y?

Example

Find gcd(143, 111)

$$143 = 1 \times 111 + 32$$
$$111 = 3 \times 32 + 15$$
$$32 = 2 \times 15 + 2$$
$$15 = 7 \times 2 + 1$$

$$\gcd(143, 110) = 1$$

$$32 = 143 - 1 \times 111$$
$$15 = 111 - 3 \times 32$$
$$= 4 \times 111 - 3 \times 143$$
$$2 = 32 - 2 \times 15$$
$$= 7 \times 143 - 9 \times 111$$
$$1 = 15 - 7 \times 2$$
$$= 67 \times 111 - 52\ 143$$

Another example

- Example: determine gcd(803; 121)
- Solution

$$
\begin{aligned}
803 &= 121.6 + 77 \\
121 &= 77.1 + 44 \\
77 &= 44.1 + 33 \\
44 &= 33.1 + 11 \\
33 &= 11.3 + 0 \\
&\rightarrow 11 = \gcd(803, 121)
\end{aligned}
$$

Extended Euclidian Algorithm

```
x=1;  y=0;  d=a;  r=0;  s=1;  t=b;
while (t>0) {
        q = ⌊d/t⌋
        u=x-qr;  v=y-qs;  w=d-qt
        x=r;     y=s;     d=t
        r=u;     s=v;     t=w
}
return (d, x, y)
```

Example

gcd(803; 121)

$$
\begin{aligned}
803 &= 121 \times 6 + 77 \\
121 &= 77 \times 1 + 44 \\
77 &= 44 \times 1 + 33 \\
44 &= 33 \times 1 + 11 \\
33 &= 11 \times 3 + 0 \\
&\rightarrow 11 = \mathrm{gcd}(803, 121)
\end{aligned}
$$

$$
\begin{aligned}
11 &= 44 - 1 \times 33 \\
&= 44 - 1 \times (77 - 1 \times 44) = 2 \times 44 - 1.77 \\
&= 2 \times (121 - 1 \times 77) - 1 \times 77 = 2 \times 121 - 3 \times 77 \\
&= 2 \times 121 - 3 \times (803 - 6 \times 121) = \mathbf{20} \times 121 - \mathbf{3} \times 803
\end{aligned}
$$

Example

$m = 841$

160^{-1} in $\mathbf{Z}_{841}$ =?

gcd(841, 160) = 1; indeed:

$$\begin{aligned}
841 &= 5 \cdot 160 + 41 \\
160 &= 3 \cdot 41 + 37 \\
41 &= 1 \cdot 37 + 4 \\
37 &= 9 \cdot 4 + 1
\end{aligned}$$

$$\begin{aligned}
1 &= 37 - 9 \cdot 4 = 37 - 9 \cdot (41 - 1 \cdot 37) \\
&= 10 \cdot 37 - 9 \cdot 41 = 10 \cdot (160 - 3 \cdot 41) - 9 \cdot 41 \\
&= 10 \cdot 160 - 39 \cdot 41 = 10 \cdot 160 - 39 \cdot (841 - 5 \cdot 160) \\
&= 205 \cdot 160 - 39 \cdot 841
\end{aligned}$$

$\leadsto 160 \cdot 205 = 1 \pmod{841} \iff 160^{-1} = 205 \pmod{841}$

The Euler Phi Function

- **Definition**

Given an integer n, $\Phi(n) = |Zn^*|$ is the number of all numbers a such that $0 < a < n$ and a is relatively prime to n (i.e., gcd(a, n)=1).

- **Theorem:** If gcd(m,n) = 1, $\Phi(mn) = \Phi(m)\,\Phi(n)$

Let p be prime, e, m, n be positive integers

1) $\Phi(p) = p-1$
2) $\Phi(p^e) = p^e - p^{e-1}$
3) If $n = p_1^{e_1} p_2^{e2} \ldots p_k^{ek}$ then

$$\Phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right)$$

Fermat's (Little) Theorem

Let p be a prime
For each integer a one has:

$$a^p = a \pmod{p}$$

and if $\gcd(p, a) = 1$:

$$a^{p-1} = 1 \pmod{p}$$

Example:
$p = 11$, $a = 2$ compute $2^{10} \pmod{11}$:

$$\begin{aligned} 2^4 &= 16 = 5 \pmod{11} \\ 2^8 &= 5^2 = 25 = 3 \pmod{11} \\ 2^{10} &= 3 \cdot 2^2 = 12 = 1 \pmod{11} \end{aligned}$$

Euler’s Theorem

- **Euler’s Theorem**
- Given integer $n > 1$, such that $\gcd(a, n) = 1$ then $a^{\Phi(n)} \equiv 1 \pmod{n}$
- **Corollary**
- Given integer $n > 1$, such that $\gcd(a, n) = 1$ then $a^{\Phi(n)-1} \bmod n$ is a multiplicative inverse of $a \bmod n$.
- **Corollary**
  - Given integer $n > 1$, x, y, and a positive integers with $\gcd(a, n) = 1$. If $x \equiv y \pmod{\Phi(n)}$, then $a^x \equiv a^y \pmod{n}$.

Linear Equation Modulo n

$$ax \equiv b \bmod n$$

- If gcd(a, n) = 1, the equation has a unique solution $x = a^{-1} b \bmod n$

Chinese Reminder Theorem (CRT)

- Theorem:

  Let $n_1, n_2, ,,, n_k$ be integers s.t. $\gcd(n_i, n_j) = 1$, $i \neq j$.

$$x \equiv a_1 \mod n_1$$
$$x \equiv a_2 \mod n_2$$
$$\ldots$$
$$x \equiv a_k \mod n_k$$

  There exists a unique solution modulo
  $n = n_1\, n_2 \ldots n_k$

Let $y_i = (n/n_i)^{-1} \bmod n_i$

Then the solution is given by $x = \Sigma_i\, x_i\, y_i\, (n/n_i) \bmod n$

Example:

$$x \equiv 5 \pmod{7}$$
$$x \equiv 3 \pmod{11}$$
$$x \equiv 10 \pmod{13}$$

- $n_1=7,\ n_2=11,\ n_3=13,\ n=1001$
- $m_1=143,\ m_2=91,\ m_3=77$
- $y_1=143^{-1} \bmod 7 = 3^{-1} \bmod 7 = 5$
- $y_2=91^{-1} \bmod 11 = 3^{-1} \bmod 11 = 4$
- $y_3=77^{-1} \bmod 13 = 12^{-1} \bmod 13 = 12$

- $x=(5\times143\times5 + 3\times91\times4 + 10\times77\times12) \bmod 1001$
  $= 13907 \bmod 1001 = 894$

Famous Number Theory Problems

FACTORING	Given n, find a factor of n
RSAP	find m such that $m^e = c$ mod n
QRP	if , decide whether a is a QR or not.
SQROOT	find x such that $x^2 = a$ mod n
DLP	find x such that $g^x = y$ mod p
GDLP	DLP on a finite cyclic group G
DHP	given g^a mod p, g^b mod p, find g^{ab} mod p
GDHP	DHP on a finite cyclic group G
SUBSETSUM	given $\{a_1, \ldots, a_n\}$ and s, find subset of a_j that sums to s