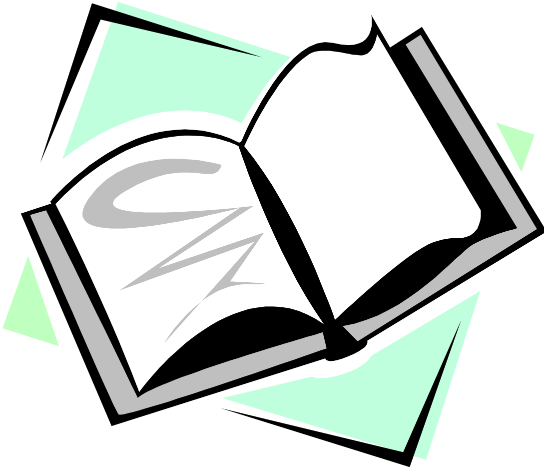
Cryptography
CS 555

Topic 12: Number Theory Basics (2)

Outline and Readings

- Outline
  - Groups
  - Residue classes
  - Euler Phi function
  - Chinese remainder theorem
- Readings:
  - Katz and Lindell: : 7.1.3, 7.1.4, 7.1.5, 7.2



Group

- A **group** is a set G along with a binary operation $\bullet$ such that the following conditions hold
  - (Closure): $\forall\, g,h \in G,\ g \bullet h \in G$
  - (Existence of an Identity):
    $\exists e \in G$ s.t. $\forall g \in G \quad g \bullet e = e \bullet g = g$
  - (Existence of inverse):
    $\forall g \in G \ \ \exists g \in G$ s.t. $\quad g \bullet h = h \bullet g = e$
  - (Associativity)
    $\forall\, g_1, g_2, g_3 \in G \quad (g_1 \bullet g_2) \bullet g_3 = g_1 \bullet (g_2 \bullet g_3)$
- Example: (Z,+), (R,+), $(Q^+,\times)$, (Permutations,Composition)

Group Concepts

- When a group G has a finite number of elements, we say that G is a **finite group**, and |G| the **order of the group**.

- We say a group is **abelian** if the following holds
  - (Commutativity:) $\forall$ g,h $\in$ G,   g • h = h • g

- We say that (H,•) is a **subgroup** of (G,•) if H is a subset of G, and (H,•) is a group
  - Find a subgroup of (Z,+)

Additive and Multiplicative Groups

- Additive group
  - Use + to denote the operation
  - Use 0 to denote the identity element
  - Use –g to denote the inverse of g
  - Use $mg = m\cdot g = g+g+\ldots+g$ (g occurs m times)
- Multiplicative group
  - Use $g\cdot h$ or simply gh to denote applying the operation
  - Use 1 to denote the identity element
  - Use g^{-1} to denote the inverse of g
  - Use g^m to denote $g \cdot g \cdot \ldots \cdot g$

Theorem 7.14

- Theorem: Let G be a finite abelian group, and $m=|G|$ be its order, then $\forall g \in G\ \ g^m=1$
- Proof.
  - Lemma: If $ab=ac$, then $b=c$.
  - Let $g_1, g_2, \ldots, g_m$ be all elements in G
  - Then $gg_1, gg_2, \ldots, gg_m$ must also be all elements in G
  - $g_1 \cdot g_2 \cdots g_m = (gg_1) \cdot (gg_2) \ldots (gg_m) = g^m\, g_1 \cdot g_2 \cdots g_m$
  - Thus $g^m=1$

Residue Classes

- Given positive integer n, congruence modulo n is an equivalence relation.
- This relation partition all integers into equivalent classes; we denote the equivalence class containing the number x to be $[x]_n$, or $[x]$ when n is clear from the context
- These classes are called residue classes modulo n
- E.g., $[1]_7=[8]_7=\{\ldots, -13,-6,1,8,15,22,\ldots\}$

Modular Arithmetic in $\mathbf{Z}_n$

- Define $\mathbf{Z}_n$ as the set of residue classes modulo n
  - $\mathbf{Z}_7 = \{[0], [1], [2], \ldots, [6]\}$
- Define two binary operators + and $\times$ on $\mathbf{Z}_n$
- Given [x], [y] in $\mathbf{Z}_n$, $[x] + [y] = [x+y]$, $[x] \times [y] = [xy]$
- E.g., in $\mathbf{Z}_7$: $[3]+[4] = [0]$, $[0]+[2] = [2]+[0] = [2]$, $[5]+[6] = [4]$
- $(\mathbf{Z}_n,+)$ is a group of size n; $(\mathbf{Z}_n,\times)$ is not a group
- Compute the table for $\mathbf{Z}_4$

Properties of Modular Addition and Multiplication

Let n be a positive integer and $\mathbf{Z}_n$ be the set of residue classes modulo n. For all a, b, c $\in \mathbf{Z}_n$

1.	$a + b = b + a$	addition is commutative
2.	$(a+b)+c = a+(b+c)$	addition is associative
3.	$a + [0] = a$	exists addition identity
4.	$[x] + [-x] = [0]$	exists additive inverse
5.	$a \times b = b \times a$	multiplication is commutative
6.	$(a\times b)\times c = a\times(b\times c)$	multiplication is associative
7.	$a\times(b+c) = a\times b+ a\times c$	mult. distributive over add.
8.	$a\times[1] = a$	exists multiplicative identity

Multiplicative Inverse

- Theorem: $[x]_n$ has a multiplicative inverse if and only if $\gcd(x,n) = 1$

- We use $\mathbf{Z}_n^*$ to denote the set of all residue classes that have a multiplicative inverse.

- What is $\mathbf{Z}_{15}^*$?

- $(\mathbf{Z}_n^*,\times)$ is a group of size $\Phi(n)$.

The Euler Phi Function

Definition

Given an integer n, $\Phi(n) = |Z_n^*|$ 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, $\Phi(mn) = \Phi(m)\,\Phi(n)$

Proof. There is a one-to-one mapping between Z_{mn}^* and $Z_m^* \times Z_n^*$

$x \rightarrow (x \bmod m, x \bmod n)$

$yn(n^{-1} \bmod m) + zm \qquad (y,z)$

The Euler Phi Function

Theorem: Formula for Φ(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

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

Fermat's Little Theorem

Fermat's Little Theorem

If *p* is a prime number and *a* is a natural number that is not a multiple of p, then

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

Proof idea: Corollary of Theorem 7.14

- gcd(a, p) = 1, then the set $\{ i \cdot a \bmod p\}$ $0< i < p$ is a permutation of the set $\{1, \ldots, p-1\}$.
  - otherwise we have $0<n<m<p$ s.t. $ma \bmod p = na \bmod p$, and thus $p \mid (ma - na) \Rightarrow p \mid (m-n)$, where $0<m-n < p$)
- $a \times 2a \times \ldots \times (p-1)a = (p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$

Since $\gcd((p-1)!, p) = 1$, we obtain $a^{p-1} \equiv 1 \pmod{p}$

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 of Theorem 7.14

Corollary

Given integer n > 1, such that gcd(a, n) = 1 then

$a^{\Phi(n)-1}$ mod n is a multiplicative inverse of a mod 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

$$a^x \equiv a^y \pmod{n}.$$

Consequence of Euler's Theorem

Principle of Modular Exponentiation

Given a, n, x, y with $n \geq 1$ and $\gcd(a,n)=1$, if $x \equiv y \pmod{\phi(n)}$, then

$$a^x \equiv a^y \pmod{n}$$

Proof idea:

$a^x = a^{k\phi(n) + y} = a^y (a^{\phi(n)})^k$

by applying Euler's theorem we obtain

$a^x \equiv a^y \pmod{p}$

Chinese Reminder Theorem (CRT)

Theorem

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

$$x \equiv a_1 \bmod n_1$$

$$x \equiv a_2 \bmod n_2$$

$$\ldots$$

$$x \equiv a_k \bmod n_k$$

There exists a unique solution modulo

$n = n_1\ n_2\ \ldots\ n_k$

Proof of CRT

- Consider the function $\chi: Z_n \rightarrow Z_{n1} \times Z_{n2} \times \ldots \times Z_{nk}$
  $\chi(x) = (x \bmod n_1, \ldots, x \bmod n_k)$
- We need to prove that χ is a bijection.
- For $1 \leq i \leq k$, define $m_i = n / n_i$, then $\gcd(m_i, n_i)=1$
- For $1 \leq i \leq k$, define $y_i = m_i^{-1} \bmod n_i$
- Define function $\rho(a1,a2,\ldots,ak) = \Sigma\ a_i m_i y_i \bmod n$, this function inverts χ
  - $a_i m_i y_i \equiv a_i \pmod{n_i}$
  - $a_i m_i y_i \equiv 0 \pmod{n_j}$ where $i \neq j$

An Example Illustrating Proof of CRT

- Example of the mappings:
  - $n_1=3$, $n_2=5$, $n=15$
  - $m_1=5$, $y_1=m_1^{-1} \bmod n_1=2$, $\quad 5\cdot 2 \bmod 3 = 1$
  - $m_2=3$, $y_2=m_2^{-1} \bmod n_2=2$, $\quad 3\cdot 2 \bmod 5 = 1$

  - $\rho(2,4) = (2\cdot 5\cdot 2 + 4\cdot 3\cdot 2) \bmod 15$
    $= 44 \bmod 15 = 14$
  - $14 \bmod 3 = 2$, $14 \bmod 5 = 4$

Example of CRT:

$x \equiv 5 \pmod 7$

$x \equiv 3 \pmod{11}$

$x \equiv 10 \pmod{13}$

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

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

Coming Attractions …

- Message Authentication Code
- Reading: Katz & Lindell: 4.1~4.4