

CS556 Introduction to Cryptography - Prof. Ming-Deh Huang

Scribe: Iftikhar A Burhanuddin

burhanud@usc.edu

Class #4 - September 5, 2002

Announcements:

Lecture notes for class #3 are online. Homework 1: § 1.1 : 6,13. § 1.2 : 11,12. § 1.3 : 1(c),5,7,10,22,24. Due Sep. 12,2002.

Topics for today:

1. Solving linear congruences
2. Subgroup generated by x , $\langle x \rangle$
3. Lagrange's theorem
4. $\phi(n)$ and the Chinese Remainder Theorem

Lecture:

Last class we had posed an exercise question: *How many solutions does the linear congruence $ax \equiv b \pmod n$ have?*

Say $d = (a, n)$ then $ax \equiv b \pmod n$ is solvable iff $d|b$. Suppose d divides b then the original linear congruence is equivalent to $a_1x \equiv b_1 \pmod{n_1}$ where $a = da_1, b = db_1, n = dn_1$. Observe that $x_0 = a^{-1}b_1 \pmod{n_1}$ is a *unique* solution to our new congruence and $x_0 + in_1, 0 \leq i \leq d - 1$ are solutions to the original. Therefore there are d solutions in all.

Subgroup generated by x , $\langle x \rangle$

Let (G, \odot) be a group and let $x \in G$. The subgroup generated by x is given by $\langle x \rangle = \{x^{(i)} \mid i \in \mathbf{Z}\}$, where

$$x^{(i)} = \begin{cases} e, & i = 0 \\ x \odot x \dots \odot x, & i > 0 \\ x^{-1} \odot x^{-1} \dots \odot x^{-1}, & i < 0 \end{cases}$$

Moreover suppose G is a finite group then $\langle x \rangle$ is finite. When we consider the powers of x , $\{x^{(1)}, x^{(2)}, x^{(3)}, \dots\}$ pigeon-hole principle tells us

that as $\langle x \rangle$ is finite all powers cannot be distinct, that is $\exists i, j \ 0 < i < j$ such that

$$\begin{aligned} x^{(j)} &= x^{(i)} \\ \Rightarrow x^{(-i)} \odot x^{(j)} &= x^{(-i)} \odot x^{(i)} \\ \Rightarrow x^{(j-i)} &= e \end{aligned}$$

So $x^{(k)} = e$ from some $k > 0$. Next we define $order(x) :=$ the least positive integer k such that $x^{(k)} = e$. Say $m = order(x)$ then $\langle x \rangle = \{e, x, x^{(2)}, \dots, x^{(m-1)}\}$. Also observe that $x^{(m)} = e \Rightarrow x^{(m-1)}x = e \Rightarrow x^{(m-1)} = x^{(-1)}$, that is negative powers fall into the same set and we can dispense with them.

Ex: $G = \mathbf{Z}/n\mathbf{Z}, H = \langle x \rangle = \{0, 3, 6, 9, 12\}$ and $4 \cdot 3 = 12 = -3 = 3 \cdot (-1)$ in the group G . Also notice that the size of the subgroup $|\langle x \rangle| = 5$ divides the size of the group $|G| = 15$ and this is no coincidence as we shall see in Lagrange's theorem but first some background.

Suppose $a, b, x \in G$ then $a \odot x = b \odot x \Leftrightarrow (a \odot x) \odot x^{-1} = (b \odot x) \odot x^{-1} \Leftrightarrow a \odot (x \odot x^{-1}) = b \odot (x \odot x^{-1}) \Leftrightarrow a = b$. The same holds true for $x \odot a = x \odot b$. Therefore we can cancel when we see the same term on either side of $=$ whenever we work with group elements.

The following map is 1 - 1 due to the cancellation argument:

$$\begin{aligned} G &\rightarrow G \\ a &\mapsto x \odot a \end{aligned}$$

Theorem (Lagrange): Suppose (G, \odot) is a finite group and (H, \odot) is a subgroup of (G, \odot) . Then $|H|$ divides $|G|$.

Proof:

Consider for $x \in G$ $xH := \{x \odot h \mid h \in H\}$

Claim 1: $|H| = |xH|$

Since

$$\begin{aligned} x \odot h &= x \odot h' \text{ for some } h, h' \in H \\ \Rightarrow x^{-1} \odot x \odot h &= x^{-1} \odot x \odot h' \\ \Rightarrow h &= h' \end{aligned}$$

The above argument establishes the injectivity. The map is clearly onto and hence is bijective. If two sets are related by a bijective map they have the same cardinality.

Claim 2: $xH, x \in G$ form a partition on G . That is for $x, y \in G$ either $xH \cap yH = \emptyset$ or $xH = yH$, in other words if the intersection is non-empty the two sets are the same. For if $\exists z \in xH \cap yH$ then $z = x \odot h_1 = y \odot h_2$ where $h_1, h_2 \in H$

$$\begin{aligned} x \odot h_1 &= y \odot h_2 \\ \Rightarrow x^{-1} \odot x \odot h_1 &= x^{-1} \odot y \odot h_2 \\ \Rightarrow h_1 &= x^{-1} \odot y \odot h_2 \\ \Rightarrow h_1 \odot h_2^{-1} &= x^{-1} \odot y \odot h_2 \odot h_2^{-1} \\ &= x^{-1} \odot y \end{aligned}$$

Let $h = h_1 \odot h_2^{-1}$. Notice that $h \in H$. $h = x^{-1} \odot y \Rightarrow x \odot h = y$
 $\forall h' \in H, y \odot h' = x \odot h \odot h_1' \in H \Rightarrow yH \subseteq xH$. Similar argument shows $yH \supseteq xH$. Therefore $yH = xH$.

Claims 1 and 2 tell us that the *cosets* of H with respect to G are disjoint and of the same cardinality. (*Note: that apart from H , the other cosets are not subgroups of G as they don't contain e .*) So $|G| = (\# \text{ of cosets}) * |H|$. In particular $|H|$ divides $|G|$. This completes the proof of Lagrange's theorem.

◇

Corollary 1: $order(x) = | \langle x \rangle |$ divides $|G|$ for all $x \in G$

Corollary 2: $x^{\phi(n)} \equiv 1 \pmod n$ for all $x \in \mathbf{Z}_{>0}$ and $(x, n) = 1$

Proof: Consider $G = (\mathbf{Z}/n\mathbf{Z}^*, *)$ which is called the multiplicative group $\text{mod } n$. We saw last class that $|G| = \phi(n)$. So for all $x \in G$ that is $x \in \mathbf{Z}_{>0}$ and $(x, n) = 1$, $order(x)$ divides $|G| = \phi(n)$ by corollary 1. Say $order(x) = k$. So $\phi(n) = km$ for some m . Hence $x^k \equiv 1 \pmod m \Rightarrow x^{\phi(n)} = (x^k)^m \equiv 1 \pmod n$ ◇

Corollary 3 - Fermat's Little Theorem (Flt):

$x^{p-1} \equiv 1 \pmod p$ for all $x \in \mathbf{Z}_{>0}$ and $p \nmid x$

Proof: Say p is a prime. By corollary 2, $x^{\phi(p)} \equiv 1 \pmod p$ for all $x, p \nmid x$, which implies $x^{p-1} \equiv 1 \pmod p$ ◇

Ex: $p = 31, x = 7, 7^{30} \equiv 1 \pmod{31} \Rightarrow 31 | (7^{30} - 1). p = 101, x = 100, 101 | (100^{100} - 1)$

Flt is equivalent to $\forall x, x^p \equiv x \pmod p$. This is true for all x so that $p \nmid x$ due to Flt and for all x such that $p | x$ trivially.

Remark: RSA encryption/decryption functions are maps from multiplica-

tive group modulo m to itself that respect multiplication modulo n

$$\begin{aligned} \mathbf{Z}/n\mathbf{Z}^* &\rightarrow \mathbf{Z}/n\mathbf{Z}^* \\ x &\mapsto x^e \bmod n =: E(x) \\ y &\mapsto y^e \bmod n \\ (x.y) &\mapsto (x.y)^e \bmod n \\ &= x^e.y^e \bmod n \end{aligned}$$

That is $E(xy) = E(x).E(y)$ in $\mathbf{Z}/n\mathbf{Z}^*$. The RSA encryption map is more than just a function it is a group homomorphism infact it is a group isomorphism demonstrated by the above *multiplicative* nature of $E(x)$.

$order(x)$ divides $\phi(n)$ by Lagrange's theorem. So $x^{\phi(n)} \equiv 1 \bmod n$. Suppose $ed \equiv 1 \bmod \phi(n)$ then $E(x)^d \bmod n = x^{ed} \bmod n = x^{1+\phi nk} \equiv x \bmod n$. This is the underlying design of the RSA cryptosystem and it's a simple but interesting play with $\mathbf{Z}/n\mathbf{Z}^*$.

$\phi(n)$ and the Chinese Remainder Theorem:

For prime p , $\phi(p) = p - 1$ and

$$\begin{aligned} \phi(p^e) &= |\{x \mid 1 \leq x \leq p^e - 1, (x, p^e) = 1\}| \\ &= p^e - \frac{p^e}{p} \\ &= p^{e-1}(p - 1) \end{aligned}$$

An interesting property of ϕ is that it is a multiplicative function, that is, if $(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$

Let $n = \prod_i p_i^{e_i}$ then

$$\begin{aligned} \phi(n) &= \prod_i \phi(p_i^{e_i}) \\ &= \prod_i p_i^{e_i-1}(p_i - 1) \\ &= n \prod_i (1 - \frac{1}{p_i}) \end{aligned}$$

We know that $\phi(n) < n$. But how much less? If n is the product of two large primes then $\prod_i (1 - \frac{1}{p_i})$ is very close to 1.

Say $x < 35$ and $x \equiv 2 \bmod 7$, $x \equiv 4 \bmod 5$. What is the solution? By eyeballing the system of congruences we know that the answer is 9. More generally let $M = m_1.m_2 \dots m_k$

$$(**) \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k} \\ (m_i, m_j) \text{ for all } i, j, i \neq j \end{cases}$$

Question: What is the smallest non-negative integer solution to (**)?

Idea: Instead of solving a big problem let's solve k problems which are easier to solve. For $1 \leq i \leq k$

$$x_i \equiv \begin{cases} a_i \pmod{m_i} \\ 0 \pmod{m_j} \quad j \neq i \end{cases}$$

Then $X = \sum_{i=1}^k x_i$ is a solution and $X = \sum_{i=1}^k x_i \pmod{M}$ is the smallest non-negative integer.

For all j

$$\begin{aligned} X &\equiv \sum_i x_i \pmod{m_j} \\ &\equiv x_j \pmod{m_j} \\ &\equiv a_j \pmod{m_j} \end{aligned}$$

$\exists y_i, x_i = q_i y_i$ where $q_i = \prod_{j \neq i} m_j = \frac{M}{m_i}$. Notice that $(q_i, m_i) = 1$. We need $q_i y_i \equiv a_i \pmod{m_i} \Rightarrow y_i = q_i^{-1} a_i \pmod{m_i}$

The solution to (**) is unique modulo M is illustrated by the following argument. For all i suppose $y \equiv a_i \pmod{m_i}$ and $x \equiv a_i \pmod{m_i}$ then $x \equiv y \pmod{m_i} \Rightarrow m_i | (x - y)$. As $(m_i, m_j) = 1$, for all $i \neq j$ we have $M = \prod_i m_i | (x - y)$ which implies $x \equiv y \pmod{M}$.

Chinese Remainder Theorem - CRT: Given a_1, \dots, a_k (**) has a unique solution modulo $M = \prod_i m_i$

$$\begin{aligned} \mathbf{Z}/M\mathbf{Z} &\rightarrow \mathbf{Z}/m_1\mathbf{Z} * \mathbf{Z}/m_2\mathbf{Z} \dots \mathbf{Z}/m_k\mathbf{Z} \\ x &\mapsto (a_1, a_2, \dots, a_k) \\ \text{where } x &\equiv a_i \pmod{m_i} \end{aligned}$$

CRT says that the map is a bijection (1-1 and onto). The fact that ϕ is multiplicative can be seen from this theorem...you'll have to wait till next class for more.