Introduction to Cryptology

Lecture 19

Announcements

- HW6 due today
- HW7 due Thursday 4/20
- Remember to sign up for Extra Credit

Agenda

- Last time
  - More details on AES/DES (K/L 6.2)
  - Practical Constructions of CRHF (K/L 6.3)
- This time
  - Number Theory Background (K/L Chapter 8)

Modular Arithmetic

Definition of modulo:

We say that two integers a, b are congruent modulo p denoted by

$$a \equiv b \; mod \; p$$

If

$$p \mid (a - b)$$

(i.e. p divides $(a - b)$).

Modular Arithmetic

Examples: All of the following are true

$$2 \equiv 15 \; mod \; 13$$

$$28 \equiv 15 \; mod \; 13$$

$$41 \equiv 15 \; mod \; 13$$

$$-11 \equiv 15 \; mod \; 13$$

Modular Arithmetic

Operation: addition mod p

Regular addition, take modulo p.

Example: $8 + 10\ mod\ 13 \equiv 18\ mod\ 13 \equiv 5\ mod\ 13$.

Properties of Addition mod p

Consider the set Z_p of integers $\{0,1,\dots,p-1\}$ and the operation addition mod p.

- Closure: Adding two numbers in Z_p and taking mod p yields a number in Z_p.
- Identitiy: For every $a \in Z_p$, $[0+a] mod\ p \equiv a\ mod\ p$.
- Inverse: For every $a \in Z_p$, there exists a $b \in Z_p$ such that $a + b \equiv 0\ mod\ p$.
  - b is simply the negation of a ($b = -a$).
  - Note that using the property of inverse, we can do subtraction. We define $c - d\ mod\ p$ to be equivalent to $c + (-d) mod\ p$.
- Associativity: For every $a, b, c \in Z_p$: $(a + b) + c = a + (b + c) mod\ p$.

Z_p is a group with respect to addition!

Definition of a Group

A group is a set G along with a binary operation $\circ$ for which the following conditions hold:

- Closure: For all $g, h \in G$, $g \circ h \in G$.
- Identity: There exists an identity $e \in G$ such that for all $g \in G, e \circ g = g = g \circ e$.
- Inverse: For all $g \in G$ there exists an element $h \in G$ such that $g \circ h = e = h \circ g$. Such an h is called an inverse of g.
- Associativity: For all $g_1, g_2, g_3 \in G, (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

When G has a finite number of elements, we say G is finite and let $|G|$ denote the order of the group.

Abelian Group

A group G with operation $\circ$ is abelian if the following holds:

- Commutativity: For all $g, h \in G$, $g \circ h = h \circ g$.

We will always deal with finite, abelian groups.

Other groups over the integers

- We will be interested mainly in multiplicative groups over the integers, since there are computational problems believed to be hard over such groups.
  - Such hard problems are the basis of number-theoretic cryptography.
- Group operation is multiplication mod p, instead of addition mod p.

Multiplication mod p

Example:

$$3 \cdot 8 \; mod \; 13 \equiv 24 \; mod \; 13 \equiv 11 \; mod \; 13.$$

Multiplicative Groups

Is Z_p a group with respect to multiplication mod p?

- Closure—YES
- Identity—YES (1 instead of 0)
- Associativity—YES
- Inverse—NO
  - 0 has no inverse since there is no integer a such that $0 \cdot a \equiv 1 \; mod \; p$.

Multiplicative Group

For p prime, define ${Z^*}_p = \{1, \ldots, p-1\}$ with operation multiplication mod p.

We will see that ${Z^*}_p$ is indeed a multiplicative group!

To prove that ${Z^*}_p$ is a multiplicative group, it is sufficient to prove that every element has a multiplicative inverse (since we have already argued that all other properties of a group are satisfied).

This is highly non-trivial, we will see how to prove it using the Euclidean Algorithm.

Inefficient method of finding inverses mod p

Example: Multiplicative inverse of $9 \; mod \; 11$.

$$9 \cdot 1 \equiv 9 \; mod \; 11$$
$$9 \cdot 2 \equiv 18 \equiv 7 \; mod \; 11$$
$$9 \cdot 3 \equiv 27 \equiv 5 \; mod \; 11$$
$$9 \cdot 4 \equiv 36 \equiv 3 \; mod \; 11$$
$$9 \cdot 5 \equiv 45 \equiv 1 \; mod \; 11$$

What is the time complexity?

Brute force search. In the worst case must try all 10 numbers in ${Z^*}_{11}$ to find the inverse.

This is exponential time! Why? Inputs to the algorithm are $(9{,}11)$. The length of the input is the length of the binary representation of $(9{,}11)$. This means that input size is approx. $\log_2 11$ while the runtime is approx. $2^{\log_2 11} = 11$. The runtime is exponential in the input length.

Fortunately, there is an efficient algorithm for computing inverses.

Euclidean Algorithm

Theorem: Let a, p be positive integers. Then there exist integers X, Y such that $Xa + Yb = \gcd(a, p)$.

Given a, p, the Euclidean algorithm can be used to compute $\gcd(a, p)$ in polynomial time. The extended Euclidean algorithm can be used to compute X, Y in polynomial time.

We will see the extended Euclidean algorithm next class

Proving $Z^*{}_p$ is a multiplicative group

In the following we prove that every element in $Z^*{}_p$ has a multiplicative inverse when p is prime. This is sufficient to prove that $Z^*{}_p$ is a multiplicative group.

Proof. Let $a \in Z^*{}_p$. Then $\gcd(a, p) = 1$, since p is prime.
By the Euclidean Algorithm, we can find integers X, Y such that $aX + pY = \gcd(a, p) = 1$.
Rearranging terms, we get that $pY = (aX - 1)$ and so $p \mid (aX - 1)$.
By definition of modulo, this implies that $aX \equiv 1 \; mod \; p$.
By definition of inverse, this implies that X is the multiplicative inverse of a.

Note: By above, the extended Euclidean algorithm gives us a way to compute the multiplicative inverse in polynomial time.

Extended Euclidean Algorithm Example #1

Find: X, Y such that $9X + 23Y = \gcd(9,23) = 1$.

$$23 = 2 \cdot 9 + 5$$
$$9 = 1 \cdot 5 + 4$$
$$5 = 1 \cdot 4 + 1$$
$$4 = 4 \cdot 1 + 0$$

$$1 = 5 - 1 \cdot 4$$
$$1 = 5 - 1 \cdot (9 - 1 \cdot 5)$$
$$1 = (23 - 2 \cdot 9) - \big(9 - (23 - 2 \cdot 9)\big)$$
$$1 = 2 \cdot 23 - 5 \cdot 9$$

$-5 = 18 \ mod\ 23$ is the multiplicative inverse of $9\ mod\ 23$.

Extended Euclidean Algorithm Example #2

Find: X, Y such that $5X + 33Y = \gcd(5,33) = 1$.

$$33 = 6 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

$$1 = 3 - 1 \cdot 2$$
$$1 = 3 - (5 - 3)$$
$$1 = (33 - 6 \cdot 5) - \big(5 - (33 - 6 \cdot 5)\big)$$
$$1 = 2 \cdot 33 - 13 \cdot 5$$

$-13 = 20\ mod\ 33$ is the multiplicative inverse of $5\ mod\ 33$.

Time Complexity of Euclidean Algorithm

When finding $\gcd(a, b)$, the “b” value gets halved every two rounds.

Why?

Time complexity: $2\log(b)$.

This is polynomial in the length of the input.

Why?

Getting Back to ${Z^*}_p$

Group ${Z^*}_p = \{1, \ldots, p - 1\}$ operation: multiplication modulo p.

Order of a finite group is the number of elements in the group.

Order of ${Z^*}_p$ is $p - 1$.

Fermat's Little Theorem

Theorem: For prime p, integer a:

$$a^p \equiv a \; mod \; p.$$

Useful Fact

Fact: For prime p and integers a, b, If $p|a \cdot b$ and $p \nmid a$, then $p \mid b$.

Corollary of Fermat's Little Theorem

Corollary: For prime p and a such that $(a, p) = 1$:

$$a^{p-1} \equiv 1 \; mod \; p$$

Proof:

- By Fermat's Little Theorem we have that $a^p \equiv a \; mod \; p$. By definition of modulo, this means that $p \mid (a^p \; - a)$. Rearranging, this implies that $p \mid a \cdot (a^p - 1)$.
- Now, since $\gcd(a, p) = 1$, we have that $p \nmid a$. Applying "useful fact" with $a = a$ and $b = (a^p - 1)$, we have that $p \mid (a^p - 1)$.
- Finally, by definition of modulo, we have that $a^{p-1} \equiv 1 \; mod \; p$.

Note: For prime p, $p - 1$ is the order of the group ${Z^*}_p$.

Generalized Theorem

Theorem: Let G be a finite group with $m = |G|$, the order of the group. Then for any element $g \in G, g^m = 1$.

Corollary of Fermat's Little Theorem is a special case of the above when G is the multiplicative group ${Z^*}_p$ and p is prime.