Introduction to Cryptology

Lecture 18

Announcements

- HW7 due today
- Sign up for EC

Agenda

- More Number Theory!

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.

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 $5\ mod\ 33$.

Chinese Remainder Theorem

Going from $(a, b) \in Z_p \times Z_q$ to $x \in Z_N$

Find the unique $x \ mod \ N$ such that

$$x \equiv a \ mod \ p$$
$$x \equiv b \ mod \ q$$

Recall since $\gcd(p, q) = 1$ we can write

$$Xp + Yq = 1$$

Note that

$$Xp \equiv 0 \ mod \ p$$
$$Xp \equiv 1 \ mod \ q$$

Whereas

$$Yq \equiv 1 \ mod \ p$$
$$Yq \equiv 0 \ mod \ p$$

Going from $(a, b) \in Z_p \times Z_q$ to $x \in Z_N$

Find the unique $x \bmod N$ such that

$$x \equiv a \bmod p$$
$$x \equiv b \bmod q$$

Claim:

$$b \cdot Xp + a \cdot Yq \equiv a \bmod p$$
$$b \cdot Xp + a \cdot Yq \equiv b \bmod q$$

Therefore, $x \equiv b \cdot Xp + a \cdot Yq \bmod N$