Introduction to Cryptology

Lecture 19

Announcements

- HW8 is up on course webpage, due 4/24
- Sign up for EC, Current Events EC

Agenda

- More Number Theory!

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:

$$a^p \equiv a \bmod p.$$

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.

Multiplicative Groups Mod N

- What about multiplicative groups modulo N, where N is composite?
- Which numbers $\{1, \ldots, N-1\}$ have multiplicative inverses $mod\ N$?
  - a such that $\gcd(a, N) = 1$ has multiplicative inverse by Extended Euclidean Algorithm.
  - a such that $\gcd(a, N) > 1$ does not, since $\gcd(a, N)$ is the smallest positive integer that can be written in the form $Xa + YN$ for integer X, Y.
- Define $Z^*{}_N \coloneqq \{a \in \{1, \ldots, N-1\} | \gcd(a, N) = 1\}$.
- $Z^*{}_N$ is an abelian, multiplicative group.
  - Why does closure hold?

Order of Multiplicative Groups Mod N

- What is the order of ${Z^*}_N$?
- This has a name. The order of ${Z^*}_N$ is the quantity $\phi(N)$, where ϕ is known as the Euler totient function or Euler phi function.
- Assume $N = p \cdot q$, where p, q are distinct primes.
  - $\phi(N) = N - p - q + 1 = p \cdot q - p - 1 + 1 = (p-1)(q-1)$.
  - Why?

Order of Multiplicative Groups Mod N

General Formula:

Theorem: Let $N = \prod_i {p_i}^{e_i}$ where the $\{p_i\}$ are distinct primes and $e_i \geq 1$. Then

$$\phi(N) = \prod_i {p_i}^{e_i - 1}(p_i - 1).$$

Another Special Case of Generalized Theorem

Corollary of generalized theorem:

For a such that $\gcd(a, N) = 1$:

$$a^{\phi(N)} \equiv 1 \; mod \; N.$$

Another Useful Theorem

Theorem: Let G be a finite group with $m = |G| > 1$. Then for any $g \in G$ and any integer x, we have

$$g^x = g^{x \bmod m}.$$

Proof: We write $x = a \cdot m + b$, where a is an integer and $b \equiv x \bmod m$.

- $g^x = g^{a \cdot m + b} = (g^m)^a \cdot g^b$
- By "generalized theorem" we have that

$$(g^m)^a \cdot g^b = 1^a \cdot g^b = g^b = g^{x \bmod m}.$$

An Example:

Compute $3^{25}\ mod\ 35$ by hand.

$$\phi(35) = \phi(5 \cdot 7) = (5-1)(7-1) = 24$$

$$3^{25} \equiv 3^{25\ mod\ 24}\ mod\ 35 \equiv 3^{1}\ mod\ 35$$

$$\equiv 3\ mod\ 35.$$

Background for RSA

Recall that we saw last time that

$$a^m \equiv a^{m \bmod \phi(N)} \bmod N.$$

For $e \in {Z^*}_N$, let $f_e: Z_N^* \to Z_N^*$ be defined as $f_e(x) \coloneqq x^e \bmod N$.

Theorem: $f_e(x)$ is a permutation.
Proof: To prove the theorem, we show that $f_e(x)$ is invertible.
Let d be the multiplicative inverse of $e \bmod \phi(N)$.
Then for $y \in Z_N^*$, $f_d(y) \coloneqq y^d \bmod N$ is the inverse of f_e.

To see this, we show that $f_d(f_e(x)) = x$.
$f_d(f_e(x)) = (x^e)^d \bmod N = x^{e \cdot d} \bmod N = x^{e \cdot d \bmod \phi(N)} \bmod N = x^1 \bmod N = x \bmod N$.

Note: Given d, it is easy to compute the inverse of f_e
However, we saw in the homework that given only e, N, it is hard to find d, since finding d implies that we can factor $N = p \cdot q$.
This will be important for cryptographic applications.