Introduction to Cryptography CS 355

Lecture 21

Group & Testing Prime Numbers

Lecture Outline

- Group
- Quadratic Residues
- Primality Test

Groups

Definition:

A group $(G, *)$ is a set G on which a binary operation $*$ is defined which satisfies the following axioms:

- Closure: For all $a, b \in G$, $a * b \in G$.
- Associative: For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
- Identity: $\exists\, e \in G$ s.t. for all $a \in G$, $a * e = a = e * a$.
- Inverse: For all $a \in G$, $\exists\, a^{-1} \in G$ s. t. $a * a^{-1} = a^{-1} * a = e$.

Definition:

A group $(G, *)$ is called an abelian group if $*$ is a commutative operation:

Commutative: For all $a, b \in G$, $a * b = b * a$.

Examples

- Is (Z, +) a group?
- Is (Z,×) a group?
- Is (Q*, ×) a group, where Q* denote non-zero rational numbers?
- The group $(Z_2,+)$
  - {0,1}
  - 0+0=0 0+1=1 1+0=1 1+1=0
  - add modulo 2 is the same as the XOR operator
- Is $(Z_{26},+)$ a group?

Modular Multiplication

- Is $(Z_7^*,\times)$ a group?
  - elements: $Z_7^*=\{1,2,3,4,5,6\}$
  - does the closure property hold?
  - does the associative property hold?
  - is there an identity element, if so, which one?
  - is there an inverse for every element? If so, what is the inverse for 3?
- Is $(Z_{26}^*, \times)$ a group?
- When is $(Z_n^*, \times)$ a group?

Cyclic Group

- Definition: Given a group $(G,\bullet)$,
  - the order of G is $|G|$
  - the order of an element a in G is the smallest positive integer such that $a^m=1$
  - $\{a,a^2,\ldots,a^m\}$ is a subgroup of G
    - (why?)
- Definition: a group $(G,\bullet)$ is a cyclic group if there exists $g\in G$ such that $G=\{g, g\bullet g, g^3, \ldots, g^{|G|}\}$
  - g is known as a generator
  - the order of g is $|G|$
    - (why?)

Z_p* is a Cyclic Group

- Fact: Given a prime p, Z_p* is a cyclic group.
  - we won't prove it here.
- There exists $g \in Z_p^*$ s.t. $\{g^j \mid 1 \le j \le p-1\} = Z_p^*$
  - g is a generator of Z_p*,
  - g is also known as the primitive element modulo p
  - what is the order of g
- For example, 2 is a generator for Z_{11}*
  - $\{2^j \mid 1 \le j \le p-1\} = \{2,4,8,5,10,9,7,3,6,1\}$
  - what is the order of $4=2^2$? what is the order of $8=2^3$?
- Let g be a generator of Z_p*, and let $a=g^j$
  - the order of a is (p-1)/gcd(p-1,j)
  - what are the primitive elements in Z_{11}*?

Quadratic Residues Modulo A Prime

Definition

- a is a quadratic residue modulo p if $\exists$ b $\in Z_p^*$ such that $b^2 \equiv$ a mod p,
- otherwise when a$\neq$0, a is a quadratic nonresidue
- Q_p is the set of all quadratic residues in Z_p^*
- $\overline{Q}_p$ is the set of all quadratic nonresidues in Z_p^*
- If p is prime there are (p-1)/2 quadratic residues in Z_p^*, $|Q_p|$ = (p-1)/2

Example

$Z_{11}^* = \{$	2,	4,	8,	5,	10,	9,	7,	3,	6,	1	$\}$
	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	

$Z_{11}^* = \{$	1,	2,	3,	4,	5,	6,	7,	8,	9,	10$\}$
Square	1	4	9	5	3	3	5	9	4	1

$$Q_{11} = \{ 1, 4, 9, 5, 3 \}$$

$$\overline{Q_{11}} = \{ 2, 6, 7, 8, 10 \}$$

How Many Square Roots Does an Element in Q_p has

- A element a in Q_p has exactly two square roots
  - a has at least two square roots
    - if $b^2 \equiv a \bmod p$, then $(p-b)^2 \equiv a \bmod p$
  - a has at most two square roots in Z_p^*
    - if $b^2 \equiv a \bmod p$ and $c^2 \equiv a \bmod p$, then $b^2 - c^2 \equiv 0 \bmod p$
    - then $p \mid (b+c)(b-c)$, either b=c, or b+c=p

Legendre Symbol

- Let p be an odd prime and a be an integer. The Legendre symbol is defined

$$\left(\frac{a}{p}\right) = \begin{cases} 0, \text{ if } p \mid a \\ 1, \text{ if } a \in Q_p \\ -1, \text{ if } a \in \overline{Q}_p \end{cases}$$

- The remaining slides in this lecture are advanced topics and won’t be in the quizs/exams

Euler's Criterion

Theorem: If $a^{(p-1)/2} \equiv 1 \bmod p$, then a is a quadratic residue (if $\equiv -1$ then a is a quadratic nonresidue)

I.e., the Legendre symbol $\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p$

Proof. If $a = y^2$, then $a^{(p-1)/2} = y^{(p-1)} = 1 \pmod p$

If $a^{(p-1)/2}=1$, let $a = g^j$, where g is a generator of the group Z_p^*. Then $g^{j\,(p-1)/2} = 1 \pmod p$. Since g is a generator, $(p-1) \mid j\,(p-1)/2$, thus j must be even. Therefore, $a=g^j$ is QR.

Jacobi Symbol

- let n ≥ 3 be odd with prime factorization

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

- the Jacobi symbol is defined to be

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \dots \left(\frac{a}{p_k}\right)^{e_k}$$

- the Jacobi symbol can be computed without factoring n

Euler Pseudo-prime

- For any prime p, the Legendre symbol $\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p$
- For a composite n, if the Jacobi symbol $\left(\frac{a}{n}\right) = a^{(n-1)/2} \bmod n$ then n is called an Euler pseudo-prime to the base a,
  – i.e., a is a "pseudo" evidence that n is prime
- For any composite n, the number of "pseudo" evidences that n is prime for at most half of the integers in Z_n^*

The Solovay-Strassen Algorithm

Solovay-Strassen(n)

choose a random integer a s.t. $1 \le a \le n-1$

$x \leftarrow \left(\frac{a}{n}\right)$

if x=0 then return ("n is composite") // gcd(x,n)$\neq$1

$y \leftarrow a^{(n-1)/2} \bmod n$

if (x=y) then return ("n is prime")

// either n is a prime, or a pseudo-prime

else return ("n is composite")

// violates Euler's criterion

If n is composite, it passes the test with at most ½ prob. Use multiple tests before accepting n as prime.

Rabin-Miller Test

- Another efficient probabilistic algorithm for determining if a given number n is prime.
  - Write n-1 as $2^k m$, with m odd.
  - Choose a random integer a, 1 = a = n-1.
  - $b \leftarrow a^m \bmod n$
  - if b=1 then return “n is prime”
  - compute b, $b^2, b^4, \ldots, b^{2^{(k-1)}}$, if we find -1, return “n is prime”
  - return “n is composite”
- A composite number pass the test with ¼ prob.
- When t tests are used with independent a, a composite passes with $(1/4)^t$ prob.
- The test is fast, used very often in practice.

Why Rabin-Miller Test Work

Claim: If the algorithm returns "n is composite", then n is not a prime.

Proof: if we choose a and returns "n is composite", then

- $a^m \neq 1$, $a^m \neq -1$, $a^{2m} \neq -1$, $a^{4m} \neq -1$, …, $a^{2^{k-1}m} \neq -1$ (mod n)
- suppose, for the sake of contradiction, that n is prime,
- then $a^{n-1} = a^{2^{k}m} = 1$ (mod n)
- then there are two square roots modulo n, 1 and -1
- then $a^{2^{k-1}m} = a^{2^{k-2}m} = a^{2m} = a^m = 1$ (contradiction!)
- so if n is prime, the algorithm will not return "composite"

Coming Attractions …

- Attacks on RSA