6.857 Rivest
3/4/09 L9.1

Admin:

Outline: Number theory & number-theoretic groups

- ☐ Divisors & GCD algorithm
- ☐ multiplicative inverses using extended gcd alg.
- ☐ orders of elements; Euler's theorem
- ☐ generators & discrete logarithms (DLP)
- ☐ finding generators
- ☐ public key crypto based on DLP
- ☐ number-theoretic groups

GCD

- d is a divisor of a if $d \geq 0$ & $d \mid a$
- $d \mid a \equiv a$ is a multiple of $d \equiv (\exists k)\ a = d \cdot k$ "d divides a"
- $(\forall d)\ d \mid 0$ $(\forall a)\ 1 \mid a$
- If d is a divisor of a & d is a divisor of b, then d is a common divisor of a & b.
- The greatest common divisor of a & b is the largest of their common divisors. [But $\gcd(0,0)=0$ by defn.]
- Ex: $\gcd(24,30)=6$ $\gcd(5,0)=5$
  $\gcd(33,12)=3$
- Def: a & b are relatively prime if $\gcd(a,b)=1$
- Euclid's alg for $\gcd(a,b)$ $[a,b \geq 0]$

$$\gcd(a,b) = \begin{cases} a & \text{if } b=0 \\ \gcd(b, a \bmod b) & \text{else} \end{cases}$$

- Ex: $\gcd(7,5)$
  $= \gcd(5,2)$
  $= \gcd(2,1)$
  $= \gcd(1,0)$
  $= 1$
- Thm $(\forall a,b)(\exists x,y)\ ax+by=\gcd(a,b)$
- Proof by example:

$$\left.\begin{aligned} 7 &= 7\cdot 1 + 5\cdot 0 \\ 5 &= 7\cdot 0 + 5\cdot 1 \end{aligned}\right\} \text{initial values}$$

$$2 = 7\cdot 1 + 5\cdot(-1)$$

$$1 = \underset{a}{7}\cdot\underset{x}{(-2)} + \underset{b}{5}\cdot\underset{y}{3}$$

[Running time is polynomial; essentially $\lg(a)\cdot\lg(b)$ bit operations]

Modular inverses

Suppose $a \in Z_p^*$ $\quad 1 \le a < p$ & $\gcd(a,p)=1$ $\quad$ (p prime?)

How to compute $a^{-1} \pmod p$?

$$a^{-1} \equiv a^{p-2} \pmod p \quad \text{if } p \text{ is prime}$$

Otherwise:

Find x, y s.t. $ax + py = 1$

$$ax = 1 \pmod p$$

$$x = a^{-1} \pmod p$$

[E.g. $5^{-1} \equiv 3 \pmod 7$]

Orders of elements (in Z_n^*)

Recall: $(\forall a \in Z_p^*)\ a^{p-1} \equiv 1 \pmod p$ $\quad$ [Fermat's Little Theorem]

In general: $|Z_n^*| = |\{a : \gcd(a,n)=1\}| = \varphi(n)$

e.g. $Z_{10}^* = \{1,3,7,9\}$ $\quad \varphi(10)=4$

If p prime, then $Z_p^* = \{1,2,\ldots,p-1\}$ & $\varphi(p)=p-1$.

Thm: [Euler] $(\forall n)\ a^{\varphi(n)} \equiv 1 \pmod n$

Def: $\text{order}_n(a)$ = "order of a, modulo n"
= least positive t s.t. $a^t \equiv 1 \pmod n$.

Example: mod 7

	1	2	3	4	5	6	7	…	
1	1	1	1	1	1	1	1	…	order(1) = 1
2	2	4	1	2	4	1	2	…	order(2) = 3
3	3	2	6	4	5	1	3	…	order(3) = 6
4	4	2	1	4	2	1	4	…	order(4) = 3
5	5	4	6	2	3	1	5	…	order(5) = 6
6	6	1	6	1	6	1			order(6) = 2

← Fermat

Def: $\langle a \rangle = \{a^i : i \geq 0\}$ subgroup generated by a

Thm: $\text{order}(a) = |\langle a \rangle|$ $\left(\langle 2 \rangle = \{2, 4, 1\} \right)$

Thm: $\text{order}_p(a) \mid p-1$ p prime

Thm: $\underbrace{|\langle a \rangle|}_{\text{order}_n(a)} \mid \underbrace{|Z_n^*|}_{\varphi(n)}$ general

Def: If $\text{order}(g) = p-1$ then g is a <u>generator</u> of Z_p^*.
(i.e. $\langle g \rangle = Z_p^*$)

Thm: If g is a generator mod p, then

$$g^x = y \pmod p$$

has a <u>unique</u> soln x, $0 \leq x < p-1$, for each $y \in Z_p^*$.

x is the "discrete log" of y, base g, modulo p.

<u>Thm:</u> $\mathbb{Z}_n^*$ has a generator $\underbrace{\ }_{\text{(i.e. } \mathbb{Z}_p^* \text{ is cyclic)}}$ iff
n is
$2, 4, p^m$, or $2p^m$ for prime p & $m \geq 1$.

<u>Thm:</u> If p is prime, # generators modulo p is $\varphi(p-1)$

E.g. $p = 11$

$|\mathbb{Z}_p^*| = \varphi(11) = 10$ $\quad \mathbb{Z}_p^* = \{1, 2, \ldots, 10\}$

how many generators?

$\varphi(10) = 4$

generators are $2, 6, 7, 8$

<u>How to find them?</u>

In general, requires knowledge of factorization of $p-1$.

<u>Def:</u> p is a "safe prime" (Sophie Germain) if
$p = 2q + 1$ (for q prime)

<u>Ex:</u> $p = 2 \cdot 5 + 1$ $\quad p = 2 \cdot 29 + 1$

$p = 2 \cdot 11 + 1$

$p = 2 \cdot 23 + 1$

If p is a "safe prime" then $\text{order}_p(a) \in \underbrace{\{1, 2, q, 2q\}}_{\text{divisors of } p-1}$

g is a generator mod $p = 2q+1$

if $g^{p-1} = 1$ ($\checkmark$ by Fermat: no need to check)

& $g^2 \neq 1$

& $g^q \neq 1$ $\Big\}$ check it

Thm: If p is prime, then

$$\varphi(p-1) = \#\text{generators mod } p \geq \frac{p-1}{6 \ln\ln(p-1)}$$

(i.e., they are dense, in general)

Thm: If p is "safe" prime, then

$$\varphi(p-1) = \#\text{generators mod } p$$
$$= q-1$$

(almost half of them!)

Generate & test works very well!

Common public-key setup:

- Public system parameters: p large prime (1024 bits)
  g generator mod p
- Alice chooses x $0 \le x < p-1$ as her <u>secret key</u>
- Alice publishes $y = g^x \pmod{p}$ as her <u>public key</u>
- Secrecy of x protected by difficulty of computing <u>discrete logs</u>

$$\log_{g,p}(y) = x$$

- Commonly assumed that DLP (discrete log problem) is infeasible, for p large & random, or p s.t. $p-1$ has large prime factor (e.g. p = safe prime).
- About as hard as to factor # of same size as p. (Empirical statement, not a theorem.)

Crypto groups:

- $Z_p^* = \{a : 1 \le a < p\}$ $\quad |Z_p^*| = p-1$

  often $p = 2r+1$, r prime, p = "safe prime"

  always "cyclic": $(\exists g)\ \langle g \rangle = Z_p^*$

  $\equiv (\forall a \in Z_p^*)(\exists k)\ g^k = a$

- Q_p = quadratic residues mod p $\quad \subsetneq Z_p^*$

  $= \{a^2 : 1 \le a < p\}$

  $|Q_p| = \frac{1}{2}|Z_p^*| = \frac{p-1}{2}$

  cyclic: if $\langle g \rangle = Z_p^*$, then $\langle g^2 \rangle = Q_p$

  $Q_p = \{ g^{2i} : 0 \le i < (p-1)/2 \}$

  If $p = 2r+1$: $|Q_p| = r$ & any element in $Q_p \ne 1$ generates Q_p

- $Z_n^* = \{a : \gcd(a,n) = 1 \ \&\ 1 \le a < n\}$

  $|Z_n^*| \triangleq \varphi(n)$

  if $n = p \cdot q$ & p, q distinct odd primes: Z_n^* not cyclic

  $Z_n^* \approx Z_p^* \times Z_q^*$ (CRT)

- $Q_n = \{a^2 : 1 \le a < n \ \&\ \gcd(a,n) = 1\}$

  if $n = pq$ (distinct odd primes): $p = 2r+1$, $q = 2s+1$

  $|Q_n| = rs$

  Q_n is cyclic