TOPIC: 6.857 - Computer & Network Security

DATE: 3/18/13

FILE UNDER:

PAGE: L12.1

Admin:

Project proposals due Friday.

Today:

Group Theory:

- ☐ Order of elements
- ☐ Generators
- ☐ PK setup
- ☐ Five common groups

TOPIC:

DATE:

FILE UNDER:

Order of elements (in $\mathbb{Z}_p^*$ or $\mathbb{Z}_n^*$):

Define: $\text{order}_n(a)$ = "order of a, modulo n"

= least $t > 0$ s.t. $a^t \equiv 1 \pmod{n}$

Recall Fermat's Little Theorem:

If p prime, then $(\forall a \in \mathbb{Z}_p^*)\ a^{p-1} \equiv 1 \pmod{p}$

For general n, we have Euler's Theorem:

$(\forall n)(\forall a \in \mathbb{Z}_n^*)\ a^{\varphi(n)} \equiv 1 \pmod{n}$

where $\mathbb{Z}_n^* = \{a : \gcd(a,n) = 1\}$

= multiplicative group modulo n

$\varphi(n) = |\mathbb{Z}_n^*|$

Example: $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$

$\varphi(10) = 4$

$3^4 \equiv 1 \pmod{10}$

Thus $\varphi(n)$ is well-defined for all n, &

$\text{order}_n(a)$ is also well-defined.

Can we say more?

TOPIC:

DATE:

FILE UNDER:

Example: mod $p = 7$

	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	6 …	order(6) = 2

Fermat

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

<u>Example:</u> $\langle 2 \rangle = \{2, 4, 1\}$ (in $\mathbb{Z}_7^*$)

<u>Theorem:</u> $\text{order}(a) = |\langle a \rangle|$

<u>Theorem:</u> If p prime: $\text{order}_p(a) \mid (p-1)$.

<u>Theorem:</u> $|\langle a \rangle| \mid |\mathbb{Z}_n^*|$

or: $\text{order}_n(a) \mid \varphi(n)$ equivalently.

TOPIC:

DATE:

FILE UNDER:

Generators

Def: If $\text{order}_p(g) = p-1$

then g is a generator of Z_p^*.

(i.e. $\langle g \rangle = Z_p^*$)

Theorem: If p is a prime and

g is a generator mod p, then

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

has a unique solution x $(0 \le x < p-1)$

for each $y \in Z_p^*$.

Def: x is the "discrete logarithm"

of y, base g, modulo p.

x	=	1	2	3	4	5	6
g^x	=	3	2	6	4	5	1

for $g=3$, modulo 7.

TOPIC:

DATE:

FILE UNDER:

Theorem: $\mathbb{Z}_n^*$ has a generator (i.e. $\mathbb{Z}_n^*$ is cyclic) iff n is

$$2,\ 4,\ p^m,\ \text{or } 2p^m$$

for some prime p & $m \geq 1$.

Theorem: If p is prime, the number of generators mod p is $\varphi(p-1)$

Example: $p = 11$

$\mathbb{Z}_{11}^*$ has $\varphi(10) = 4$ generators (they are 2, 6, 7, and 8).

How to find a generator mod a prime p?

In general, seems to require knowledge of factorization of $p-1$.

While factoring is hard, we can create primes for which factoring $p-1$ is trivial.

TOPIC:

DATE:

FILE UNDER:

Def: If p & q are both primes &

$$p = 2q + 1$$

then p is a "safe prime" and

q is a "Sophie Germain prime".

Examples: $p = 23,\ q = 11$ $\qquad$ $p = 11,\ q = 5$

$p = 59,\ q = 29$ $\qquad$ ...

Theorem: If p is a safe prime

then $p - 1 = 2 \cdot q$

so $(\forall a \in \mathbb{Z}_p^*)$ $\text{order}_p(a) \in \{1, 2, q, 2q\}$.

It is not hard to find safe primes. ("Probability" that a prime p is safe is $\approx 1/\ln(p)$, empirically.)

Can test if g is a generator mod $p = 2q + 1$ easily:

check that $g^{p-1} = 1 \pmod p$ $\quad$ ✓ by Fermat

& $g^2 \neq 1 \pmod p$ $\quad$ $[\text{order}_p(g) \neq 2]$

& $g^q \neq 1 \pmod p$ $\quad$ $[\text{order}_p(g) \neq q]$

then $\text{order}_p(g) = p - 1$.

TOPIC:

DATE:

FILE UNDER:

We can use "generate & test" again: (for "safe prime" p)

$$\begin{aligned} &\underline{\text{do}} \quad g \xleftarrow{R} \mathbb{Z}_p^* \\ &\underline{\text{until}} \quad \text{order}_p(g) = p-1 \end{aligned}$$

Generators are quite common:

__Theorem:__ If $p = 2q+1$ is a "safe prime"

then # generators mod p

$= \varphi(p-1)$

$= q - 1$ (almost half of them!)

(In general:

__Theorem:__ If p prime, then

generators mod p

$= \varphi(p-1)$

$\geq \dfrac{p-1}{6 \ln\ln(p-1)}$

)

So generate & test works well for finding generators modulo a safe prime p, or modulo any prime p for which you know $\varphi(p-1)$.

- **Common public-key setup:**

  Public system parameters

p	large prime	(e.g. 1024 bits)
g	generator mod p	

  Alice choose x $\quad 0 \le x < p-1$ as her secret key.

  Alice publishes $y = g^x \pmod p$ as her public key.

- Secrecy of x protected by difficulty of computing discrete log

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

- Commonly assumed that discrete log problem (DLP) is infeasible for p large & random, or p large safe prime.

  (Appears to be roughly as hard as factoring a large integer of the same size as p. This is observation, not a theorem.)