Group Theory

Tuesday, September 5, 2017 12:29 PM

Today:

- Groups
- Programming w/ Groups
- Crypto Egg Challenge

$\mathbb{Z}^+$ +: closed in $\mathbb{Z}$

identity: 0

inverse: $-x$

$\mathbb{Z}_n$ (integers modulo n)

$\{0, 1, \dots n-1\}$

$a + b \mod n$

$|\mathbb{Z}_5| = 5$

Ex. $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$2 + 3 \mod 5 = 0$

$inv(2) = 3$

$\mathbb{Z}_n^*$ Ex. $\mathbb{Z}_5^*$ $\{1, 2, 3, 4\}$

$1^{-1} = 1$

$2^{-1} = 3$ $3 \cdot 2 = 6 = 1 \mod 5$

$4^{-1} = 4$ $4 \cdot 4 = 16 = 1 \mod 5$

0

$\mathbb{Z}_6^* = \{1, \cancel{2}, \cancel{3}, \cancel{4}, 5\}$

$\cancel{2}^{-1} = ?$

$5^{-1} = 5$ $5 \cdot 5 = 25 = 1 \mod 6$

$\mathbb{Z}_n^*$ group of integers mod n relatively prime with n

$\mathbb{Z}_p^*$ where p prime $\{1, \dots p-1\}$ $|\mathbb{Z}_p^*| = p-1$

Algebra hierarchy

Magma: closed binary op

Semigroup: magma w/ associative

monoid: semigroup w/ identity.

group: monoid w/ inverses

Subgroups

$(G, \cdot)$ is a subgroup of $(H, \cdot)$

if $G \subseteq H$ and

G is a group.

Ex: $\mathbb{Z}_6^{+}$ ← mod 6 does it have any subgroups?

$\{0, 1, 2, 3, 4, 5\}$

How about $\{0\}$

$\{0, 1\}$? no

$\{\}$ no

$2 = |\{0, 3\}|$? closed ✓
identity ✓
$3^{-1} = 3$, $3+3 = 0 \bmod 6$ ✓

$3 \stackrel{\checkmark}{=} \{0, 2, 4\}$ closed inverses

Theorem: [LaGrange]

If G is subgroup oh H,

then $|G|$ divide $|H|$

$$\langle g \rangle := \{ g^x \mid x \in \mathbb{N} \}$$

$$g^{\overset{x \in \mathbb{N}}{x}} = \underbrace{g \cdot g \cdots g}_{x \text{ times}} \qquad g \in G$$

Claim: $\langle g \rangle$ is a subgroup.

— closed

$$g^a \cdot g^b \overset{?}{\in} \langle g \rangle$$
$$= g^{(a+b)} \in \langle G \rangle \checkmark$$

— inverse

$$(g^a)^{-1} \;?\qquad |\langle g \rangle| \leq |G|$$

Claim: $\exists n, \; g^n = e$

$$(g^a)^{-1} = g^{(n-a)} \qquad g^a \cdot g^{(n-a)} = g^n = e$$

Cosets

Defn: Let G be a subgroup of H.
Let $h \in H$.
The h-coset of G is
$\{hg \mid g \in G\}$

Ex: $\mathbb{Z}_6^+ = \{0,1,2,3,4,5\} \leftarrow H$
$\{0,2,4\} \leftarrow G$
1-coset of G: $\{1+0, 1+2, 1+4\}$
$\quad\quad 1 \quad 3 \quad 5$

Claim: Cosets form an equivalence relation on H

Define $a \sim b$ $\quad aG = bG$
- symmetric $\quad aG = bG \Rightarrow bG = aG$
- transitive $\quad aG = bG, bG = cG \Rightarrow aG = cG$
- reflexive $\quad aG = aG$

$\mathbb{Z}_6$ $\quad 0, 2, 4$
$\quad\quad 1, 3, 5$

Lemma: Bijection between cosets.

domain $\rightarrow$ $\leftarrow$ codomain

$\phi_{a,b} : aG \rightarrow bG$ $\qquad \phi^{-1}_{a,b}$

$\phi(x) = b(a^{-1})x$

$x \in aG \Rightarrow x = ag$ for some $g \in G$

$a^{-1}x \in G$

$b(a^{-1})x \in bG$

$\phi^{-1}_{a,b}(x) = ab^{-1}(x)$

So, $|aG| = |bG|$

Therefore $|G| \,\big|\, |H|$

(divides)

Corollaries relevant to crypto:

1. If $|G|$ is prime

$\Rightarrow$ No nontrivial subgroups!

$g \in G \Rightarrow \langle g \rangle = G$ if $g \neq e$

g is a generator of G

If $|G|$ prime, Every element (except e) is a generator

Safe rimes

p is a "safe prime"
if $p = 2q+1$ and q is prime

$\mathbb{Z}_p^*$ $|\mathbb{Z}_p^*| = 2q$

safe prime

Suppose $g \in \mathbb{Z}_p^*$.

Is g in a subgroup of size q?

Fact: $g^{|G|} = e$ $g^{|G|} \in \langle g \rangle$

$g^{q \cdot 2} = (g^2)^q = e$

If $g^2 \neq e$
and $g^q = e$,
then $|\langle g \rangle| = q$

Schnorr subgroup:
$G < \mathbb{Z}_p^*$, $\underset{=2q+1}{p}$ safe prime, $|G| = q$

Discrete Log Problem:

given g, generator of G,
and $X \xleftarrow{\$} G$ sample uniform random
find x s.t. $X = g^x$

| orithm: repeated squaring

Given $x \in \mathbb{N}$, g,
Compute g^x?
1. Compute g, g^2, g^4, g^8
$(g^2)^2$
2. represent x as $x_0, x_1, \ldots$ binary rep
$g^{x_0} \cdot (g^2)^{x_1} \cdot (g^4)^{x_2} \cdot \ldots$