Crash course in modern algebra

Recap: goal for now: key exchange secure against eavesdropping.
can't be done efficiently with sym. crypto.
Need algebra. First example: Diffie-Hellman key exchange.
Today: background & a modern view.

Let's get started: modular arithmetic

- n: positive integer, p: a positive prime.

Notation: $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ add, sub, mul mod n.

note: $-3 \bmod 15 = 12$

Fact (Euclid, 200BC): For all ints. n, m there exist ints. a, b

s.t. $a \cdot n + b \cdot m = \gcd(n, m)$

$$\boxed{\text{moreover, } a, b \text{ can be found using } O(\log(n+m)) \text{ add/sub/div2 using Euclid's alg. (quadratic alg.)}}$$

ex: $\gcd(12, 18) = 6$ $\quad \underbrace{\boxed{2}}_{a} \times 12 \; \underbrace{\boxed{-1}}_{b} \times 18 = 6$

$\gcd(n, m) = 1 \Rightarrow n$ & m are relatively prime.

Modular inversion: over rationals: inverse of 2 is $\frac{1}{2}$. What about $\mathbb{Z}_n$?

Def: the <u>inverse</u> of $x \in \mathbb{Z}_n$ is $y \in \mathbb{Z}_n$ s.t. $x \cdot y = 1$ in $\mathbb{Z}_n$.

y is denoted x^{-1}.

ex: n an odd integer. Then 2^{-1} in $\mathbb{Z}_n$ is $y = \frac{n+1}{2}$.

$2 \cdot \frac{n+1}{2} = n+1 = 1$ in $\mathbb{Z}_n$.

Which element in $\mathbb{Z}_n$ have an inverse?

Lemma: x in $\mathbb{Z}_n$ has an inverse $\iff \gcd(x,n) = 1$.

Proof: $\gcd(x,n) = 1 \Rightarrow \exists a,b \in \mathbb{Z} : a \cdot x + b \cdot n = 1$

$\Rightarrow a \cdot x = 1$ in $\mathbb{Z}_n \Rightarrow x^{-1} = a$ in $\mathbb{Z}_n$

constructive: quadratic time alg. for finding inverse!

$\gcd(x,n) > 1 \Rightarrow \forall a \in \mathbb{Z}: \gcd(a \cdot x, n) > 1$

remainder mod n can't be 1 $\Rightarrow a \cdot x \neq 1$ in $\mathbb{Z}_n \Rightarrow$ no inverse. ∎

Notation: $\mathbb{Z}_n^* = $ (set of invertible elements in $\mathbb{Z}_n$)

$= \{0 \le x < n : \gcd(x,n) = 1\}$

ex: $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \dots, p-1\}$ size $= p-1$.

$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ size $= 4$

For $x \in \mathbb{Z}_n^*$ can find x^{-1} in time $O(\log^2 n)$.

solving modular linear equations:

solve $a \cdot x + b = 0$ in $\mathbb{Z}_n$

$\Rightarrow$ $x = -b \cdot a^{-1} \in \mathbb{Z}_n$ run time: $O(\log^2 n)$

same for systems of lin. eq: Gaussian elim.

what about quadratic & cubic equations ??

The structure of $\mathbb{Z}_p^*$

Thm (Fermat 1640): Let p be a prime.

$\forall x \in \mathbb{Z}_p^*$: $x^{p-1} = 1$ in $\mathbb{Z}_p$

ex: $p = 5$: $3^4 = 81 = 1$ in $\mathbb{Z}_5$

App:

(1) $x \in \mathbb{Z}_p^* \Rightarrow x \cdot x^{p-2} = 1$ in $\mathbb{Z}_p$ $\Rightarrow$ $\boxed{x^{-1} = x^{p-2} \text{ in } \mathbb{Z}_p}$

$\Rightarrow$ another way to invert in $\mathbb{Z}_p^*$, but time $= O(\log^3 p)$.

(2) to generate a (probable) 2048-bit prime:

repeat: $p \xleftarrow{R} \{2^{2047}, \dots, 2^{2048} - 1\}$

until $2^{p-1} = 1$ in $\mathbb{Z}_p$

output p

$\Pr[p \text{ not prime}]$ is small.

(3) in $\mathbb{Z}_{11}^*$: $3^{2022} = 3^{2022 \bmod 10} = 3^2 = 9$

<u>The structure thm (Euler)</u>: $\mathbb{Z}_p^*$ is a <u>cyclic group</u>

i.e.: $\exists g \in \mathbb{Z}_p^*$ s.t. $\{1, g, g^2, g^3, \dots, g^{p-2}\} = \mathbb{Z}_p^*$

such a g is called a <u>generator</u>.

ex: $p=7$ $\{1, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = \mathbb{Z}_7^*$

not all elems. are gens: $\{1, 2, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\} \subseteq \mathbb{Z}_7^*$

<u>more generally</u>: a <u>finite cyclic group</u> is a pair $(G, \cdot)$ where G is a finite set and $\cdot : G \times G \to G$ is a <u>mult. op</u> (properties: identity, inverse, associative, commutative)

moreover $\exists$ generator $g \in G$ s.t. $G = \{1, g, g^2, g^3, \dots\}$.

<u>Def</u>: For $h \in G$, $\text{order}(h) = |\{1, h, h^2, h^3, \dots\}|$

ex: in $\mathbb{Z}_7^*$: $\text{order}(3) = 6$, $\text{order}(2) = 3$.

$g \in G$ is a generator $\Longrightarrow$ $\text{order}_G(g) = |G|$.

<u>Fact</u>: $\forall g \in G$: $g^{\text{order}(g)} = 1$

<u>Thm (Lagrange)</u>: $\forall g \in G$: $\text{order}(g)$ divides $|G|$.

<u>Corollary (Fermat)</u>: $\forall g \in G$: $g^{|G|} = \left[g^{\text{order}(g)}\right]^{|G|/\text{order}(g)} = 1$

$G = \mathbb{Z}_p^*$

<u>computing roots</u>: G a finite cyclic group of <u>known</u> <u>prime</u> order q ($|G| = q$) with generator $g \in G$.

ex: $G = \langle g \rangle \subseteq \mathbb{Z}_p^*$.

<u>Problem</u>: given $h \in G$ and $1 < e < q$ find $y = h^{1/e}$ (i.e. $y^e = h$)

<u>alg</u>:
(1) compute $\alpha := (e^{-1} \bmod q) \in \mathbb{Z}_q$
(2) output $y := h^\alpha \in G$

why? $\alpha \cdot e = 1$ in $\mathbb{Z}_q$ $\Rightarrow \exists k \in \mathbb{Z}$ s.t. $\alpha \cdot e = 1 + kq$

$$\boxed{y^e} = (h^\alpha)^e = h^{1+kq} = h \cdot (h^q)^k = \boxed{h}.$$

<u>note</u>: this works when q is <u>known</u> and <u>$\gcd(e, q) = 1$</u>.

$\Rightarrow$ can compute square roots, cube roots, etc.

<u>examples</u>:

- computing $\sqrt{h}$ when q is odd:

$$\alpha = (2^{-1} \bmod q) = \frac{q+1}{2} \in \mathbb{Z} \Rightarrow \sqrt{h} = h^{\frac{q+1}{2}}$$

- computing $\sqrt[3]{h}$ when $q = 1 \pmod 3$:

$$\alpha = (3^{-1} \bmod q) = \frac{2q+1}{3} \in \mathbb{Z} \Rightarrow \sqrt[3]{h} = h^{\frac{2q+1}{3}}$$

Diffie-Hellman in cyclic groups (e.g. $\mathbb{Z}_p^*$ or E.C.)

G finite cyclic group of order q w/ gen $g \in G$.

A	(G, q, g)	B
$\alpha \xleftarrow{R} \mathbb{Z}_q$ $\{0,1,2,\dots,q-1\}$	$\xrightarrow{A = g^\alpha}$	$\beta \xleftarrow{R} \mathbb{Z}_q$
	$\xleftarrow{B = g^\beta}$	
	$\text{key} = g^{\alpha\beta} \in G$	

Security: eavesdropper sees g, g^α, g^β wants $g^{\alpha\beta}$.

<u>Def</u>: The <u>comp. D-H</u> (CDH) assump. holds in (G, g) if:

$\forall$ "eff" adv. $\mathcal{A}$ $\quad \Pr[\mathcal{A}(g, g^\alpha, g^\beta) = g^{\alpha\beta}]$ is "neg"

when $\alpha, \beta \xleftarrow{R} \mathbb{Z}_q$.

Current examples: (1) $\mathbb{Z}_p^*$ $\qquad$ (2) Elliptic curve over $\mathbb{Z}_p$

best CDH alg. (GNFS) $\qquad$ best CDH alg

time $\approx e^{\sqrt[3]{\ln(p)}}$ $\qquad$ time $= \sqrt{p} \approx e^{\frac{1}{2}\cdot\ln p}$

p must be ≥ 2048 bits. $\qquad$ p can be 256 bits

A related problem: the discrete log problem in G

Problem: given $h \in G$ find $\alpha \in \mathbb{Z}_q$ s.t. $h = g^\alpha$.

ex in $\mathbb{Z}_{11}^*$: Dlog base 2

h	1	2	3	4	5	6	7	8	9	10
$\mathrm{Dlog}(h)$	0	1	8	2	4	9	7	3	6	5

Like logarithms, but in finite group.

Def: The DLOG-assump. holds in (G, g) if:

$\forall$ "eff" adv. A $\Pr[A(g, g^\alpha) = \alpha]$ is "neg" when $\alpha \xleftarrow{R} \mathbb{Z}_q$.

examples: $\mathbb{Z}_p^*$ and ell. curve over $\mathbb{Z}_p$.

Fact: DLOG easy $\Rightarrow$ CDH easy

$[g, g^\alpha, g^\beta \rightarrow g^{\alpha\beta}]$ use DLOG alg. to find α.

The converse: CDH easy $\Rightarrow$ DLOG easy

is known to be true for some groups

$\Rightarrow$ no shortcut for CDH w/o computing DLOG.

<u>Thm</u>: (Euler) let $\varphi(n) = |\mathbb{Z}_n^*|$ (e.g. $\varphi(12) = |\{1,5,7,11\}| = 4$)

Then: $\forall x \in \mathbb{Z}_n^* : x^{\varphi(n)} = 1$ in $\mathbb{Z}_n$

<u>ex</u>: (1) p prime $\Rightarrow$ $\varphi(p) = |\mathbb{Z}_p^*| = p-1 \Longrightarrow$ Fermat

(2) $n = p \cdot q$ product of two distinct primes $\Rightarrow$ $\varphi(n) = (p-1)(q-1)$

$$\forall x \in \mathbb{Z}_n^* : x^{(p-1)(q-1)} = 1 \text{ in } \mathbb{Z}_n$$

(3) $5^{\varphi(12)} = 5^4 = 625 = 1$ in $\mathbb{Z}_{12}$.

computing $\varphi(n) = |\mathbb{Z}_n^*|$ is as hard as factoring n.

$\Rightarrow$ w/o factorization of n,

computing e'th roots in $\mathbb{Z}_n^*$ is belived to be difficult.

(For $e > 1$)