Cryptography using finite cyclic groups

Math basics.

Modular Arithmetic:

n positive integer, p, q: positive primes

notation: $\mathbb{Z}_n$: $\{0 \ldots n-1\}$

add, sub, modify modulo n

note: $-3 \bmod 15 = 12$.

Fact: (Euclid, 200 BC)

For all ints $n, m > 0$, there exist other ints a, b

s.t. $an + bm = \gcd(n, m)$

Moreover, a, b can be found using $O(\log(n+m))$ adds, subs, div 2 using Euclid's alg.

ex. $\gcd(12, 18) = 6$

$$\underset{a}{\underset{\uparrow}{2}} \times 12 + \underset{b}{\underset{\uparrow}{(-1)}} \times 18 = 6$$

Def. $\gcd(n, m) = 1 \iff n, m$ relatively prime.

Modular inverses: the inverse of $x \in \mathbb{Z}_n$ is $y \in \mathbb{Z}_n$

s.t. $x \cdot y = 1$ in $\mathbb{Z}_n$

ex. n odd int, 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 elements in $\mathbb{Z}_n$ have inverses?

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

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

$\Rightarrow ax=1$ in $\mathbb{Z}_n$

$\Rightarrow x^{-1}=a$.

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

$\Rightarrow ax \neq 1$ in $\mathbb{Z}_n$

$\Rightarrow x$ has no inverse.

use Euclid's alg to compute x^{-1} in $\mathbb{Z}^n$ in $O(\log^2 n)$

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

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

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

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

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

Solving modular linear equations.

Solve $ax+b=0$ in $\mathbb{Z}_n$, $a \in \mathbb{Z}_n^*$

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

Runtime $O(\log^2 n)$

System of linear modular eq.

$\Rightarrow$ Solve using Gaussian elimination.

Quadratic 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 $\mathbb{Z}_5$

Application: generating a $\underline{\underline{\text{probable}}}$ 2048-bit prime

repeat:

$p \xleftarrow{R} \{2^{2047} \ldots 2^{2048}-1\}$

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

output p

Interview q: in $\mathbb{Z}_{11}^*$: $3^{2022} = (3^{202})^{10} \cdot 3^2$

$= (1^{202})^{10} \cdot 3^2 = 9$

$$\boxed{3^x = 3^{x \bmod p-1} \text{ in } \mathbb{Z}_p}$$

The structure thm of $\mathbb{Z}_p^*$ (Euler):

$\mathbb{Z}_p^*$ is a finite cyclic group

($\exists g \in \mathbb{Z}_p^*$ st $\{1, g, g^2, \ldots, g^{p-2}\} = \mathbb{Z}_p^*$

such a g is called a generator.)

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

$\quad\quad 3^0 \; 3^1 \; 3^2 \; 3^3 \; 3^4 \; 3^5$

$\Rightarrow$ 3 is generator.

More generally: a finite cyclic group is a pair $(\underbrace{G}_{\text{finite set}}, \cdot)$

$\cdot : G \times G \to G$
multiplication op.

w/ identity, inverse,
associativity, commutativity

Moreover: $\exists$ generator $g \in G$. st.

$$G = \{1, g, g^2, g^3, \ldots\}$$

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

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

$\quad\quad \text{order}(2) = 3$

g generator of $G \Leftrightarrow \text{order}(g) = |G|$.

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

Thm (Lagrange): $\forall g \in G$: order(g) divides $|G|$

Corollary (Fermat): $\forall g \in G$: $(G = \mathbb{Z}_p^*)$ $\quad g^{p-1} = g^{|G|}$

$$= [g^{\text{order}(g)}]^{|G|/\text{order}(g)}$$

Computing roots:

G is a finite cyclic group of known prime order

w/gen $g \in G$ ($|G|$ prime)

ex. fix prime p

choose element $h \in \mathbb{Z}_p^*$

s.t. $\mathrm{order}(h) = q$, prime q

Problem: given $h \in G$, $1 < e < q$

find $y = h^{1/e}$

(i.e. $y^e = h$)

algorithm: (1) compute $\alpha := e^{-1} \bmod q$

(2) output $y := h^{\alpha} \in G$

why $y^e = h$?

$\alpha \cdot e = 1$ in $\mathbb{Z}_q \Rightarrow \exists k \in \mathbb{Z}: \alpha \cdot e = 1 + kq$

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

Computing exponents in FCG

let G be an FCG of order q

Input: $h \in G$, $x \in \mathbb{Z}$

Output: $h^x \in G$

Algorithm: repeated squaring alg.

$z \leftarrow 1$, $y \leftarrow h$

for $i = 0 \ldots n$:

if $x_i = 1$ set $z \leftarrow zy \in G$

$y \leftarrow y^2 \in G$

output z

$O(\log|G|)$ multiplications in g (each $O(\log^2|G|)$ time)

$\Rightarrow O(\log^3|G|)$ ops