Factorization

Monday, March 29, 2021 8:40 AM

Recall: RSA

$n = p \cdot q \Rightarrow \phi(n) = (p-1)(q-1)$

Quadratic Residues

SQRT Problem: $\sqrt{a} \pmod n$

$\Rightarrow$ NP-Hard problem for composite n

$\Rightarrow$ if n is prime, or its prime factors are known, then Sqrt is easy.

1] Euler's Criterion:

if c is QR in mod p then

$$c^{(p-1)/2} \equiv 1 \pmod p$$

$c \in Q_p$

$\Rightarrow x^2 \equiv c \pmod p$

$c^{(p-1)/2} \equiv x^{p-1} \equiv 1$

e.g. in $\mathbb{Z}_{101}^*$, is $55 \in Q_{101}$?

Sol. Test: $55^{100/2} \equiv 55^{50} \equiv 100 \not\equiv 1$

$\therefore$ 55 is QNR in (mod 101)

2] Solve $\sqrt{c} \pmod p$, for prime $p \equiv 3 \pmod 4$

$$\left(\pm \underbrace{c^{(p+1)/4}}_{x}\right)^2 \equiv c^{(p+1)/2}$$

$$\equiv c^{(p-1)/2} \cdot c^{2/2}$$

$$\equiv 1 \cdot c^1 \quad \text{by E.C.}$$

$$\equiv c \pmod p$$

$\therefore$ $\boxed{\sqrt{c} \equiv \pm c^{(p+1)/4} \pmod{p}}$, for $p \equiv 3 \pmod 4$

for $p \equiv 1 \pmod 4$ (HW)

3] e.g. in $\mathbb{Z}_{13}^*$

① Does $\sqrt{11}$ exist or not?

Sol. check if 11 is QR.

by E.C. $11^{(13-1)/2} \equiv 11^6 \equiv (-2)^6 \equiv -1 \not\equiv 1 \Rightarrow$ QNR

② $\sqrt{5}$?

by E.C. $5^6 \equiv (25)^3 \equiv (-1)^3 \equiv -1 \Rightarrow$ QNR $\Rightarrow$ no root.

③ $\sqrt{3}$?

by E.C. $3^6 \equiv (3^5)^2 \equiv (1)^2 \equiv 1 \Rightarrow$ QR

4] e.g. In $\mathbb{Z}_{19}^*$, find $\sqrt{15}$ if possible

by E.C., $15^{(19-1)/2} \equiv 15^9 \equiv (-4)^9 \equiv -2^{18} \equiv -1 \Rightarrow$ QNR

② find $\sqrt{4}$ if possible

by E.C. $4^9 \equiv 1 \Rightarrow$ QR

$\therefore \sqrt{4} = \pm 4^{(19+1)/4} \equiv \pm 4^5 \equiv \pm 2^{10} \equiv \pm 2 \equiv 2, 17$

5] Integer Factorization Problem

5] Integer factorization Problem

Given an integer m (of length n-bits; $m < 2^n$), find the prime factorization of m.

i.e. write m as $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_t^{e_t}$, where p_i is prime.

e.g. $m = 180$

Factorization of $m \Longrightarrow m = 2^2 \cdot 3^2 \cdot 5^1$

2	180
2	90
3^2	45
5	

e.g. $m = 391$

$\Rightarrow m = 17 \cdot 23$

6] Factorization is a hard problem.

in particular: when $m = p \cdot q$ for large primes p, q

7] factorization Algorithms: (assame n-bit integer)

① Trial division algorithm

for $i = 2$ to $\sqrt{m}$, try m/i $\quad m \approx 2^n$

$\Rightarrow$ Time complexity: $O(\sqrt{m}) = O(2^{n/2}) \Rightarrow$ Exponential.

② General number field sieve (GNFS) algorith

best known algorith to factorize integers on classical computers (deterministic algorith)

Time complexity: $O\left(e^{cn^{1/3}\log^{2/3}n}\right) \cong \left(2^{O(\sqrt[3]{n})}\right)$

subexponential.

8] In practice, $n \geq 1000$ bits

e.g. RSA

8] In practice, n = 1000 bits

e.g. RSA

9] Factorization is reduced to Sqrt : factorization $\leq_p$ Sqrt.

idea : $\sqrt{y} \longrightarrow x$, $x^2 = y$

① Choose random $r \in \mathbb{Z}_m^*$

② $y = r^2 \pmod m$

③ $x = \sqrt{y} \pmod m$

④ if $x \equiv \pm r \pmod m$

Go to ①

else

$p = \gcd(x \pm r, m)$

$q = m/p$;

return (p, q)

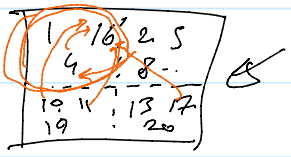
e.g. $m = 3 \cdot 7 = 21$

$\sqrt{16} \pmod{21}$

$\sqrt{16} \equiv 4, 17, 10, 11$

$\phi(21) = 12$

$\frac{12}{4} = 3$



$y = r^2 \pmod m$

$y - r^2 \equiv 0 \pmod m$

$(\sqrt{y} - r)(\sqrt{y} + r) \equiv 0 \pmod m$

$m \mid (x - r)(x + r)$

10] e.g. factorize $m = 21$

$\sqrt{1} = 1, -1, 8, 13$

$y - 1^2 \equiv 0 \pmod{21}$

$(8 - 1)(8 + 1) \equiv 0 \pmod{21}$

$\mathbb{Z}_{21}^*$

$\gcd(8 - 1, 21) = 7$

$\gcd(8 + 1, 21) = 3$

} factors of 21