NUMBER THEORY

We will introduce some concrete assumptions: FACTORING, DISCRETE LOG, LEARNING WITH ERRORS.

Number Theory is about modular arithmetic, i.e. mod n, namely

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

Then you can have structures like

$(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n, +, \cdot)$

$+, \cdot$ are mod n.

For instance $(\mathbb{Z}_n, +)$ is a GROUP.
The situation is different for $(\mathbb{Z}_n, \cdot)$, it is not always a group.

LEMMA If $\gcd(a, n) > 1$, then $a \in \mathbb{Z}_n$ not invertible mod n w.r.t. "$\cdot$".

Made with Goodnotes

Proof. Say a is INVERTIBLE: $\exists\, b \in \mathbb{Z}_n$ s.t. $a \cdot b = 1 \mod n$. Then:

$$ab = 1 + q \cdot n \quad \text{for } q > 0.$$

Now, $\gcd(a, n)$ must divide also $ab - qn$, which means it also divides 1. Or, $\gcd(a, n) = 1$. $\boxtimes$

On the other hand, we'll see that if $\gcd(a, n) = 1$, then a is invertible.

Made with Goodnotes

This motivates the following def :

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

$$\# \mathbb{Z}_n^* \triangleq \varphi(n)$$

↳ EULER TOTIENT FUNCTION.

Some special cases :

$n = p =$ a prime

$$\mathbb{Z}_p^* = \{ 1, \dots, p-1 \} \; ; \; \underset{\varphi(p) = p-1}{\overset{\# \mathbb{Z}_p^*}{\parallel}}$$

$n = p \cdot q$ with p, q primes.

But we'll see $\varphi(n) = (p-1)\cdot(q-1)$
$$\varphi(n) = \# \mathbb{Z}_n^*$$
(We'll show this later.)

We are interested in doing efficiently operations over $\mathbb{Z}_n^*$ or $\mathbb{Z}_p^*$ for pretty large n or p (e.g. $|p|$ is 2048 bits)

Something easy: Addition and multi-

plication can be done in polynomial time. In fact $O(\log^2 n)$.
We now show, that the inverse can also be computed in polynomial time.
This is possible using the EXTENDED EUCLIDEAN ALGORITHM.

LEMMA Let a, b s.t. $a \geq b > 0$. Then
$\gcd(a, b) = \gcd(b, a \bmod b)$.

Proof. We have $a = q \cdot b + a \bmod b$
with $q = \lfloor a/b \rfloor$.

Made with Goodnotes

Now: a common divisor of a and b is also a divisor of $a \bmod b = a - qb$.

Similarly, a common divisor of $a \bmod b$ and b also divides $a = qb + a \bmod b$ $\boxtimes$

THM Given $a \geq b > 0$ we can compute $\gcd(a, b)$ in poly-time. Also, we can compute u, v s.t.

$$\gcd(a, b) = au + bv$$

Cor. Assuming $\gcd(a, n) = 1$, we can compute in polynomial time u, v s.t.

$$1 = \gcd(a, n) = a \cdot u + n \cdot v$$

$$\Longrightarrow \quad a \cdot u = 1 \mod n$$

u is the inverse.

Example: $a = 14$, $b = 10$. Then:

$$14 = 1 \cdot 10 + 4$$

$$10 = 2 \cdot 4 + 2$$

$$\Rightarrow \gcd(14, 10) = 2$$

$$4 = 2 \cdot 2 + 0$$

Moreover:

$$2 = 10 - 2 \cdot 4 = 10 - 2 \cdot (14 - 1 \cdot 10)$$

$$= \underbrace{3}_{v} \cdot 10 + \underbrace{(-2)}_{u} \cdot 14$$

Dim. We apply the lemma recursively:

$$a = b q_1 + r_1 \qquad 0 \leq r_1 < b$$

and $\gcd(a, b) = \gcd(b, r_1)$. Then:

$$b = r_1 \cdot q_2 + r_2 \qquad 0 \leq r_2 < r_1$$

$\to r_1 \bmod r_2$

$$r_1 = r_2 \cdot q_3 + r_3$$

$r_n \bmod r_{n+1}$

$\dots$

$$r_i = q_{n+2} r_{n+1} + \underset{}{\overset{\shortparallel}{r_{n+2}}}$$

$$\Rightarrow \gcd(a, b) = \gcd(b, r_1) = \cdots$$

$$= \cdots = \gcd(r_t, r_{t+1})$$

$$= r_t$$

when $r_{t+1} = 0$.

It remains to show that t is polynomial in $|b| = \lambda$.

Clearly, $r_{i+1} < r_i$. But we can show $r_{i+2} \leq r_i / 2$.

If $r_{i+1} \leq r_i/2$ then it's immediate.

So assume $r_{i+1} > r_i/2$. But:

$$r_{i+2} = r_i \bmod r_{i+1}$$

$$= r_i - q_{i+2} r_{i+1}$$

$$< r_i - r_i/2$$

$$= r_i/2 \qquad \blacksquare$$

$\approx$ 2λ steps !!

What about exponentiation?

$$a^b = a^{\sum_{i=0}^{t} b_i \cdot 2^i} \mod n$$

$$= \prod_{i=0}^{t} a^{b_i \cdot 2^i} \mod n$$

$$= a^{b_0} \cdot (a^2)^{b_1} \cdot (a^4)^{b_2} \cdot \ldots \cdot (a^{2^t})^{b_t} \mod n$$

binary representation: $b = (b_t \, b_{t-1} \ldots b_0)$

Complexity: $O(\log^3 \lambda)$

We also need to understand: prime numbers. Luckily there are MANY PRIMES.

THM (PRIME NUMBER THEOREM).

$$\pi(x) = \text{"\# primes} \leq x\text{"}$$

$$\geq \frac{x}{3 \log_2 x} \simeq x / \log x$$

Assuming we can test primality (which we can), then we can generate

λ-bit random primes:

- Sample $x \leftarrow [2^\lambda - 1]$ and test if prime.
- If not, repeat.

$$\Pr[\text{No output in } t \text{ steps}] \le \left(1 - \frac{1}{3\lambda}\right)^t \le (1/e)^\lambda$$

for $t = 3\lambda^2$.

Made with Goodnotes

THM (Miller-Rabin '80, AKS '02).

We can test if a λ-bit value is prime in poly(λ) time.

The main idea behind this algorithm uses this theorem:

THM. For all $a \in \mathbb{Z}_n^*$ we have:

$$a^b = a^{b \bmod \varphi(n)} \mod n$$

$$a^{\varphi(n)} = 1 \mod n$$

EULER THM.

$(a^{p-1} = 1 \mod p$ if p is prime$)$

FERMAT LITTLE THM.

Fermat Test:

- Given n, compute $a^{n-1} \mod n$.
  - If not 1 output NOT PRIME.
- Else output MAYBE PRIME.

Doesn't it work:

- There are n not prime s.t.

$$a^{n-1} = 1 \mod n$$

(FERMAT LIARS)

- There are n not prime s.t.

$$a^{n-1} = 1 \mod n \quad \forall a \in \mathbb{Z}_n^*$$

(CARMICHAEL NUMBERS)

Proof. On the one hand:

$$e^b = e^{q \cdot \varphi(m) + b \bmod \varphi(m)}$$

$$= \underbrace{\left(e^{\varphi(m)}\right)}_{1 \text{ by Euler's Theorem}}{}^{q} \cdot e^{b \bmod \varphi(m)}$$

$$= e^{b \bmod \varphi(m)}$$

The second part follows by Lagrange:
If $\mathbb{H}$ is a subgroup of G, then

$$|\mathbb{H}| \mid |G| .$$

Now $(\mathbb{Z}_m^*, \cdot)$ is a group with $\varphi(m)$ elements. Consider the subgroup:

$$\underset{\underset{1}{\parallel}}{a^0}, a^1, a^2, \ldots\ldots, a^{d-1}, \underset{\parallel}{a^d}$$

Let d be the order?.

Then by Lagrange the order d is s.t. $d \cdot k = \varphi(n)$

$$\Rightarrow \quad a^{\varphi(n)} \equiv (a^d)^k \equiv 1 \mod n.$$

$\blacksquare$

Let $n = p$ a prime. We know that $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ is CYCLIC.

$\exists \ g \in \mathbb{Z}_p^*$ s.t.

$$\mathbb{Z}_p^* = \{g^0, g^1, g^2, \ldots, g^{p-2}\}$$

Made with Goodnotes

EXAMPLE: 3 is a generator of $\mathbb{Z}_7^*$

but 2 is NOT.

$\{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\} \bmod 7$

$= \{1, 3, 2, 6, 4, 5\}$

$$3^6 \equiv 3^{p-1} \equiv 1 \mod p$$

Instead $2^3 \equiv 1 \mod 7$. It generates a subgroup.