NUMBER THEORY

We want to convince ourselves that certain operations can be performed EFFICIENTLY

Mainly work over $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$

for large n (e.g. $|n| = 2048$ bits).

- → Addition and multiplication are ok.
  (the schoolbook algorithms) $O(\log^2 n)$.
- → Inverse? In particular, multiplicative.

LEMMA. If $\gcd(a, n) > 1$, then a NOT invertible.

How to compute the inverse?

$$\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n : a \text{ invertible mod } n \}$$

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

E.g., $n = p$ a PRIME. Then $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$

$$\varphi(p) = p - 1.$$

For us, it will be important $n = p \cdot q$ (p, q PRIMES).

$$\varphi(n) = (p-1) \cdot (q-1).$$

LEMMA Let a, b s.t. $a \geq b > 0$. Then:

$$\gcd(a,b) = \gcd(b, a \bmod b).$$

Proof. We have $a = q \cdot b + r = q \cdot b + a \bmod b$.

$\Rightarrow$ A common divisor of a and b is also

common divisor of $a - qb = a \bmod b$.

Symmetrically, common divisor of b and $a \bmod b$ is

also common divisor of $a = q \cdot b + a \bmod b$ ∎

THM. Given a, b, we can compute $\gcd(a,b)$ in poly time.

Also, we can find u, v s.t. $\gcd(a,b) = au + bv$.

Application: $b = n$, assume $\gcd(a, n) = 1$.

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

$$1 \equiv a \cdot u \pmod{n}$$

$$\Rightarrow u = a^{-1} \mod n.$$

Proof. Use the lemma recursively:

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

and $\gcd(a, b) = \gcd(b, r_1)$. Do it again:

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

...

Stop when $r_{t+1} = 0$. Then:

$$\gcd(a,b) = \gcd(b, r_1) = \gcd(r_1, r_2)$$

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

(E.g. $a = 14$, $b = 10$

$14 = 1 \cdot 10 + 4$ ← r_1 ; $10 = 2 \cdot 4 + 2$ ← r_2

$4 = 2 \cdot 2 + 0$ ← r_3 $\Rightarrow \gcd(14,10) = 2$

u, v: $2 = 10 - 2 \cdot 4 = 10 - 2(14 - 10)$

$= (-2) \cdot 14 + 3 \cdot 10$

$u = -2$

$v = 3$)

To finish the proof, note that $r_{i+1} < r_i$

but this is not enough.

But, we can show $r_{i+2} \le r_i / 2 \quad \forall\ 0 \le i \le t-2$

$\Rightarrow$ # of steps $\approx 2\lambda$

If $r_{i+1} \le r_i / 2$ then is nothing to prove.

(because $r_{N+2} < r_{i+1} \le r_i / 2$).

So, $r_{i+1} > r_i / 2$. In fact, $r_i > r_{i+1} > r_i / 2$

$\Rightarrow$ $r_{i+2} = r_i \bmod r_{i+1} = r_i - q_{i+2}\, r_{i+1}$

$r_1 = r_2 q_3 + r_3$

$\le r_i - r_{i+1} < r_i - r_i/2 = r_i/2$ ☒

Exponentiation : $a^b \bmod m$.

SQUARE-AND-MULTIPLY : $b = (b_\ell, b_{\ell-1}, \dots, b_0)$

$$a^b \equiv a^{\sum_{i=0}^{\ell} b_i 2^i} \equiv \prod_{i=0}^{\ell} a^{b_i \cdot 2^i}$$

$$\equiv a^{b_0} \cdot (a^2)^{b_1} \cdot (a^4)^{b_2} \cdot \dots \cdot (a^{2^\ell})^{b_\ell}$$

a, a^2, a^4

$b = 1\ 1\ 0$

$a^2 = res$; $res = res \cdot a^4 \cdot res$

Primes. Few things we need:

THM There are infinite primes and

$$\pi(x) = \text{"\# of primes} \le x\text{"} \geq \frac{x}{3\log x} \approx \frac{x}{\log x}$$

$$\Pr_x\left[x \text{ prime} : x \in [2^{\lambda-1}]\right] \geq \frac{2^{\lambda-1}}{3\log(2^{\lambda}-1)} \Big/ 2^{\lambda-1}$$

$$\approx 1/3\lambda$$

Repeating t times wrongful w.p. $\leq \left(1-\frac{1}{3\lambda}\right)^t \Big/ t = 3\lambda^2 \quad \left(\approx e^{-\lambda}\right)$

Requires to test if n is PRIME.

THM (Miller-Rabin '80, AKS '02). We can test in poly time if n is prime $\clubsuit$.

We also need:

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

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

$$a^{\varphi(n)} = 1 \pmod n \longrightarrow \text{EULER THEOREM}$$

$$a^{p-1} = 1 \pmod p \longrightarrow \text{FERMAT LITTLE THEOREM}$$

$(n = p$ a PRIME$)$.

Cyclic groups: $\mathbb{Z}_p^*$, p PRIME

$\exists\ g$ the generator s.t. $\mathbb{Z}_p^* = \{ g^0, g^1, g^2, \cdots, g^{p-2} \}$

$g^{p-1} = 1 \mod p$

$\mathbb{Z}_7^*$ has generator $3 = g$ but 2 not a generator

$\{ 3^0, 3^1, 3^2, 3^3, 3^4, 3^5 \} = \{ 1, 3, 2, 6, 4, 5 \}$

$z^3 = 1 \mod 7$. FACT We can generate random primes along with generator g