Lecture 4

Last time: modular arithmetic.

$$x \bmod N = r \quad \Rightarrow \quad x = q \cdot N + r \qquad q = \left\lfloor \frac{x}{N} \right\rfloor$$

$$0 \leq r \leq N-1$$

Today:

Congruence: x is "equivalent to" y.

$\boxed{x \equiv y \bmod N}$ is defined as x and y have the same remainder when divided by N.

$x \bmod N = r$

$y \bmod N = r.$

$\Rightarrow x = Nq + r$

$- \quad y = Nq' + r.$

$x - y = N(q - q') + 0 \quad \Rightarrow x - y$ is divisible by N

$N \mid (x-y)$ notation.

$N = 3$

x	N	r
-2	3	1
1	3	1
4	3	1
0	3	0
6	3	0
		⋮

all x that gives to same r are in the equivalence class.

So how do we compute $\frac{x}{N}$ i.e. simple division.

if $\gcd(a, N) = 1$ then the Extended Euclid Algorithm gives us integers x, y s.t.

$$ax + Ny = 1 \Rightarrow ax \equiv 1 \bmod N$$
$$\Rightarrow x \text{ is } a^{-1}$$

<u>Theorem:</u> if d divides both a and b. <u>AND</u>

$ax + by = d$ for some integers x, y.

then $\gcd(a, b) = d$ ✓.

<u>why?</u> since $d \mid a$ and $d \mid b$ it is a $\underbrace{\text{common divisor}}$ (perhaps not the largest one)

So $d \le \gcd(a, b)$

Since $\gcd(a, b)$ must be a common divisor of a and b, it must also divide d.

$ax + by = d$. $\Rightarrow d \ge \gcd(a, b) \Rightarrow d = \gcd(a, b)$

so observe that if we can find such x, y that $ax + by = d$ holds then $\gcd(a, b) = d$.

To describe Euclid's Alg. we need Euclid's rule for gcd( )

$$\boxed{\begin{array}{l}\text{If } x, y \text{ are } > 0 \text{ with } x \ge y \\ \text{then } \gcd(x, y) = \gcd(x \bmod y, y).\end{array}}$$

<u>why?</u> we will prove a simpler case:

$\underline{\gcd(x, y)} = \underline{\gcd(x - y, y)} = d$

[note: the same proof will be true by subtracting y from x repeatedly.]

- If d divides both x, y also divides $(x - y)$
  $\Rightarrow \gcd(x, y) \le \gcd(x - y, y)$
- If d divides $(x - y)$ and y then also divides x, y
  $\Rightarrow \gcd(x, y) \ge \gcd(x - y, y) \Rightarrow \gcd(x, y) = \gcd(x - y, y)$

Euclid's Alg.

function Euclid (a, b)

s.t. $a \geq b \geq 0$

output $\gcd(a, b)$

If $b = 0$ return a

return Euclid$(b, a \bmod b)$

Example! $\gcd(81, 57)$

$$\underbrace{81}_{a} = 1 \cdot \underbrace{57}_{b} + \underbrace{24}_{r}$$

$$57 = 2 \cdot \underbrace{24}_{b} + 9$$

$$24 = 2 \cdot 9 + 6$$

$$9 = 1 \cdot 6 + 3$$

$$6 = 2 \cdot 3 + 0$$

$\gcd(81, 57) = 3$

Extended Euclid's Alg.

fun. ext. Euclid (a, b)

s.t $a \geq b \geq 0$

output x, y, d s.t.

$d = \gcd(a, b)$ and

$d = ax + by$

If $b = 0$ return $(1, 0, a)$

$(x', y', d) = $ ExtEuclid$(b, a \bmod b)$

return $\left(y', x' - \left\lfloor \frac{a}{b} \right\rfloor y', d\right)$

we will reverse the steps and rewrite all these equations except the last one by solving for the remainders

$r_1 = a - d q_1$

$r_2 = b - r_1 q_2$

$r_3 = r_1 - r_2 q_3$ ..

$\vdots$

$r_j = r_{j-2} - r_{j-1} q_j$

$$3 = 9 - 1 \cdot \underbrace{6}$$

$$6 = 24 - 2 \cdot \underbrace{9}$$

$$9 = 57 - 2 \cdot \underbrace{24}$$

$$81 - 1 \cdot 57$$

$$\Rightarrow 81x + 57y = 3$$

$x = -7$, $y = 10$

$\Rightarrow$ If we want to compute $57^{-1} \bmod 81$ can we do it?

what about $15^{-1} \bmod 26$

Question: does $15^{-1} \bmod 26$ exist?

fun Euclid $(26, 15)$

$26 = 1.15 + 11$

$15 = 1.11 + 4$

$11 = 2.4 + 3$

$4 = 1.3 + 1$ gcd

$3 = 3.1 + 0$

$\gcd(26, 15) = 1$

$1 = 4 - \underbrace{3}_{11 - 2.\underbrace{4}_{15 - 1.\underbrace{11}_{26 - 1.15}}}$

$1 = 3.15 - 4(26 - 15) = \underline{7.15 - 4.26}$

$$\boxed{d = x.a + b.y}$$

$7.15 = 105 = 1 + 4(26) \equiv 1 \bmod 26$

(4) Modular arithmetic: modular exponentiation

$x^y \bmod N$ each of x and y, N are n-bit #s.

$(2^n)^{2^n} \bmod N$ $x = 2^n$

Algorithm: square and reduce $x^{2\lfloor \log y \rfloor} \bmod N$

$x \bmod N \to x^2 \bmod N \to \cdots$

eg: $x^{26} = x^{16} . x^{8} . x^{2}$

$x^{26} = x^{11001_2} = x^{10000_2} . x^{1000_2} . x^{10_2}$

} $\log y$ multiplications each takes $O(\log^2 N)$ time.

$\Rightarrow$ polynomial Algorithm