Math 321

$\gcd(a,b)$ → long way $\quad a = p_1^{q_1} \cdots p_k^{q_k}$, $b = p_1^{q_1} \cdots p_k^{q_k}$ → factor to primes

$$\gcd(a,b) = p_1^{\min(q_1,b_1)} \; p_2^{\min(q_2,b_2)} \cdots p_k^{\min(q_k,b_k)}$$

Faster way?

$\gcd(a,b)$

Notice: $\boxed{a = qb + r}$ $\quad 0 \le r < b-1$

if a number divides b and r → number divides a (and b)

(vs) $\quad a - qb = r$

if a number ("d") divides a and b → number divides r (and b)

↑ says $d \mid a \wedge d \mid b$ iff $d \mid b \wedge d \mid r$ (any d)

→ $\boxed{\gcd(a,b) = \gcd(b,r)}$ Euclids Algorithm

$$a = qb + r$$

ex) $\gcd(25, 15)$

$= \gcd(15, 10)$

$= \gcd(10, 5) = 5$

$25 = (1)15 + 10$

$15 = (1)10 + \boxed{5}$ ✓

$10 = (2)(5) + (0)$ ✓

$1 = \gcd(51, 22)$

$= \gcd(22, 7)$

$= \gcd(7, 1) = 1$

$51 = 2(22) + 7$ ←

$22 = 3(7) + 1$ ←

$7 = (7)1 + 0$

$1 = (1)22 + (-3)7$

$1 = (1)22 + (-3)(51 - 2(22))$ ←

$\gcd(51,22) = 1 = (7)(22) + (-3)(51)$ ←

Bezout's thm $\gcd(a,b) = s \cdot a + t \cdot b$ ←

Def: $\gcd(a,b) = 1 \rightarrow$ call a,b **relatively prime.**

why ☞ Mult. inverse in modular arithmetic?

$3 \cdot 7 \equiv_{7} 1$

(ex) $(7)(22) + (-3)(51) = 1$ ✓ b/c $\gcd(51,22) = 1$

take mod 51 to both sides?

$(7)(22) \bmod 51 = 1$

so 7 and 22 are inverses under mod 51

$\bar{a}$ is inv. under mod m

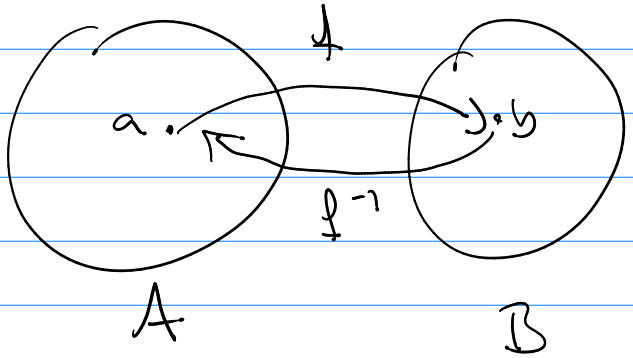
So $a \cdot \bar{a} \bmod m = 1$

① only when $\boxed{\gcd(a, m) = 1}$

② Find $\bar{a} \bmod m$ by using euclids alg. on $\gcd(a, m)$ (see above example for $\gcd(51, 22)$)

4.6 Cryptography

f must be a bijection.



a : "plain text"

b : "cypher text"

f : encryption function

f^{-1} : decryption function

---

ex) A set of all sound ideas in english

B set of all sounds ideas is spanish

→ phonogram cat

→ logogram 猫

public key (vs) private key cryptography

(1) private: $f(p) = c$

c is known (by bad guys)

and if f is known by bad guys

→ f^{-1} is "trivial" for them.

(2) public $f(p) = c$

a) c is known

b) f is known

but f^{-1} is not-trival to find knowing c and f.

How?

(1) Create a true private key

(2) Mix it up (private key → Mix → public key)

(3) $f(p)$ depends on public key

ex) private key: 2, 3 public key: $2 \cdot 3 = 6$

f uses this

Private: character ciphers (1-1 replacement)

1. shift
2. affine-shift
3. one-time-pads
4. random 1-1 replacement
5. block cipher

Public: 1. RSA - Locks