

Definition: $\text{GCD}(a, b) = X$ where X is the smallest possible integer of the form $sa+tb$ where $s, t \in \mathbb{Z}/\mathbb{N}\mathbb{Z}$

Proof:

Part 2:

Goal: $x \leq \text{GCD}(a, b)$

Implies $x|a, x|b$

Let us assume that there exists q such that $a = qx+r$

Hence $a = q(sa+tb) + r$

$$R = (1-qs)a - qtb$$

This r is a combination of a, b and $r < x$. Since x is the smallest possible combination of a, b ' r ' must be positive.

Therefore $r=0$

So $x|a$

Similarly $x|b$

Therefore $x \leq \text{GCD}(a, b)$

From both proofs $x = \text{GCD}(a, b)$

Extended Euclidean Algorithm

Consider an example with numbers 24, 33.

$$\begin{array}{l} [1 \quad 0 \quad 33] \\ [0 \quad 1 \quad 24] \\ = [1 \quad -1 \quad 9] \quad (33 + (-1)*24) \\ = [-2 \quad 3 \quad 6] \quad (24 + (-2)*9) \\ = [3 \quad -4 \quad 3] \quad (9 + (-1)*6) \\ = [-8 \quad 11 \quad 0] \quad (6 + (-2)*3) \end{array}$$

Consider the row above '0'

$$3 \cdot 33 - 4 \cdot 24 = 3$$

So GCD of 24, 33 is 3.

RSA step:

Pick e, d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$

1. Pick e randomly such that $\text{GCD}(e, (p-1)(q-1)) = 1$
2. Use extended Euclidean algorithm to find s, t such that $se + t(p-1)(q-1) = 1$

Def: $a \equiv b \pmod m \iff m \mid a-b$

$$se - 1 = -t(p-1)(q-1)$$

$$se \equiv 1 \pmod{(p-1)(q-1)}$$

So take $s=d$

Therefore $ed \equiv 1 \pmod{(p-1)(q-1)}$

Modular inverses:

Given a, m, when does there exist a, b such that $ab \equiv 1 \pmod m$ and how can we find it.

If b exists $\iff \text{GCD}(a, m) = 1$

Proof:

a) $\text{GCD}(a, m) = 1$

There exists s, t such that $sa + tb = 1$

Hence $sa \equiv 1 \pmod m$

Therefore $s=b$

b) If b exists

$$ab \equiv 1 \pmod m$$

$$ab - 1 = qm$$

$$ab - qm = 1$$

Therefore $\text{GCD}(a, m) \leq 1$ but 1 is the smallest possible GCD for any two numbers which implies

$$\text{GCD}(a, m) = 1$$

Modular exponentiation:

$$C = m^e \bmod N$$

Doing the above using e multiplications is not feasible for bigger numbers.

Instead we consider $e = \sum_{i=0}^n 2^i e_i$

$$M^e = m^{\sum_{i=0}^n 2^i e_i}$$

$$= \prod_{i=0}^n m^{2^i e_i}$$

Above problem can be done in $O(\log e)$ multiplications.

Modexp (e, x, n)

If $e = 0$

Return 1

Else $e = \text{Modexp}(m, \lfloor e/2 \rfloor, n)$

$$a = a^2 * m^{e_0} \bmod n$$

Return a

e.g.:

$$4^{13} \bmod 7$$

$$= 4^8 4^4 4^1 \bmod 7$$

$$= 2 * 4 * 4 \bmod 7$$

$$= 4 \bmod 7 = 4$$

Miller Rabin Primality test:

Observation $(N-1)^2 \equiv 1 \pmod N$

Fact: If N is prime, then only x such that $x^2 \equiv 1 \pmod N$ is $x^2 \equiv \pm 1 \pmod N$

If N is not prime, there are at least 4 numbers that square to 1 mod N

Chinese remainder theorem:

If $N=pq$ and $\gcd(p, q) = 1$

Then $Z/NZ \approx Z/pZ * Z/qZ$

$X \rightarrow (x \bmod p, x \bmod q)$

$tqa + spb \bmod N = (a, b)$

Where $sp + tq = 1$

$(a, b) \rightarrow tqa + spb \bmod N$

$\rightarrow tqa \bmod p + spb \bmod q$

$= (a \bmod p + b \bmod q)$

If p, q are prime

$(\pm 1)^2 \equiv 1 \bmod p$

$(\pm 1)^2 \equiv 1 \bmod q$

$(1 \bmod p, 1 \bmod q) \rightarrow tq + sp \equiv 1 \bmod N$

$(-1 \bmod p, -1 \bmod q) \rightarrow -tq - sp \equiv -1 \bmod N$

$(1 \bmod p, -1 \bmod q) \rightarrow tq - sp \bmod N$

$(-1 \bmod p, 1 \bmod q) \rightarrow -tq + sp \bmod N$