

Kenzley Alphonse
CSE 508
10/16/09

Topics

- Pick large primes
 - Distinguishing primes
- Modular exponentiation
- Modular inverses
- Pick e & d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$

Theorem: $\gcd(a, b) = x$ where x is the smallest positive linear combination of a & b such that $sa + tb = x$.

Proof:

- $\gcd(a, b) = x$
- Goal $x \leq \gcd(a, b)$
- Goal $x \mid a, x \mid b$

By division algorithm, $\exists q \ 0 \leq r \leq x$ such that $a = bq + r \Rightarrow a = qx + r$

$$\begin{aligned} \text{Hence } a &= q(sa + tb) + r \\ r &= (1 - qs)a + qtb \end{aligned}$$

Thus r is linear combination of a & b and $r < x$.

Since x is the smallest positive linear combination of a & b , r must not be positive.

$$\text{Hence } r = 0 \text{ so } x \mid a \Rightarrow x \mid b$$

$$\text{Hence } x \leq \gcd(a, b)$$

■

Extended Euclidean Algorithm

Example: 24 & 33

$$1 \times 33 + 0 \times 24 = 33$$

$$0 \times 33 + 1 \times 24 = 24$$

$$\left| \begin{array}{ccc} 1 & 0 & 33 \\ 0 & 1 & 24 \end{array} \right| \rightarrow \left| \begin{array}{ccc} 1 & -1 & 9 \\ 0 & 1 & 24 \end{array} \right| \rightarrow \left| \begin{array}{ccc} 1 & -1 & 9 \\ 2 & 3 & 6 \end{array} \right| \rightarrow \left| \begin{array}{ccc} 3 & -4 & 3 \\ 2 & 3 & 6 \end{array} \right| \rightarrow \left| \begin{array}{ccc} 3 & -4 & 3 \\ -8 & 11 & 0 \end{array} \right|$$

One of RSA Steps

Def: $a \equiv b \pmod{m} \Leftrightarrow m \mid a - b$

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

1. Pick e, d randomly such that $\gcd(e, (p-1)(q-1)) = 1$
2. Used Extended Euclidean Algorithm to find d such that
 - $se + t(p-1)(q-1) = 1$
 - $se - 1 = -t(p-1)(q-1)$
 - $se \equiv 1 \pmod{(p-1)(q-1)}$
3. So take $d = s$

Modular Images

Given a & m when does there exists a & b such that $ab \equiv 1 \pmod{m}$ and how can we find it.

Theorem

b exists if only if the $\gcd(a, m) = 1$. (Use Extended Euclidean Algorithm)

Proof

If $\gcd(a, m) = 1$, then $\exists s$ & t such that $sa + tm = 1$

Hence $sa \equiv 1 \pmod{m}$ so $b = s$.

Now suppose b exists then $a \cdot b \equiv 1 \pmod{m}$ so $ab - 1 = qm \Rightarrow ab - qm = 1$. Since 1 is now a linear combination of a, m $\gcd(a, m) \leq 1$. Since GCD's are always positive, $\gcd(a, m) = 1$.

Modular Exponentiation

$$c \equiv m^e \pmod{N}$$

for $i = 1 \rightarrow e$

$$a = am$$

NOT EFFECTIVE

Solution

$$e = 10011011100001$$

$$e = \sum_{i=0}^{13} 2^i e_i$$

$$m^e = m^{\sum_{i=0}^{13} 2^i e_i} = \prod_{i=0}^{13} (m^{2^i})^{e_i}$$

$$m^{2^0} = m$$

$$m^{2^1} = m^2$$

$$m^{2^2} = m^4$$

:

$$m^{2^i} = (m^{2^{i-1}})^2$$

Thus it was able to reduce to $O(\log e)$ multiples.

modexp(*m*, *e*, *N*) =

if *e* = 0

return 1

a = *modexp*(*m*, [*e*/2], *N*)

a = *a*² × *m*^{*e*} mod *N*

return *a*

Example:

$$4^{13} \text{ mod } 7$$

$$13 = 8 + 4 + 1$$

$$4^1 \equiv 4 \text{ mod } 7$$

$$4^2 \equiv 2 \text{ mod } 7$$

$$4^4 \equiv 2 \text{ mod } 7$$

$$4^8 \equiv 4 \text{ mod } 7$$

Miller-Robin Primarily Test – This test determines whether a number is prime. Since this is a Probabilistic test there is a small chance of error that if the number is composite it will tell us that the number is prime.

Observations

$$(N - 1)^2 = N^2 - 2N + 1$$

$$(N - 1)^2 \equiv 1 \text{ mod } N$$

Proof

$$N - 1 \equiv -1 \text{ mod } N \Rightarrow (N - 1)^2 \equiv (-1)^2 \text{ mod } N \equiv 1 \text{ mod } N$$

■

Fact if N is a prime, then the only x such that $x^2 \equiv 1 \pmod{N}$ is $x \equiv \pm 1 \pmod{N}$. If N is not prime, there are at least 4 numbers that squared to $1 \pmod{N}$.

Chinese Remainder Theorem

If $N = pq$ then $\gcd(p, q) = 1$, then $\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/p \times \mathbb{Z}/q$.

$$x \mapsto (x \pmod{p}, x \pmod{q})$$

These rings are isomorphic.

$$tqa + spb \pmod{N} \leftrightarrow (a, b) \text{ where } s + tq = 1$$

$$(a, b) \mapsto (tqa + spb \pmod{N})$$

$$\mapsto (tqa \pmod{p}, spb \pmod{q})$$

$$\mapsto (a \pmod{p}, b \pmod{q})$$

$$(\pm 1)^2 \equiv 1 \pmod{p}$$

$$(\pm 1)^2 \equiv 1 \pmod{q}$$

$$(1 \pmod{p}, 1 \pmod{q}) \mapsto tq + sp \equiv 1 \pmod{N}$$

$$(-1 \pmod{p}, -1 \pmod{q}) \mapsto -t - sp \equiv -1 \pmod{N}$$

$$(1 \pmod{p}, -1 \pmod{q}) \mapsto tq - sp \pmod{N}$$

$$(-1 \pmod{p}, 1 \pmod{q}) \mapsto -tq + sp \pmod{N}$$