**ALG 4.0**  
Number Theory Algorithms:

(a) GCD  
(b) Multiplicative Inverse  
(c) Fermat & Euler's Theorems  
(d) Public Key Cryptographic Systems  
(e) Primality Testing

---

**Greatest Common Divisor**

$GCD(u,v) = \text{largest } a \text{ s.t. } a \text{ is a divisor of both } u, v$

---

**Euclid's Algorithm**

```
procedure GCD(u,v)
begin
  if v=0 then return(u)
  else return (GCD(v,u mod v))
```

---

**Inductive proof of Correctness:**

if $a$ is a divisor of $u,v$

$\iff a \text{ is a divisor of } u - \left\lfloor \frac{u}{v} \right\rfloor v = u \mod v$
Time Analysis of Euclid's Algorithm for n bit numbers \(u, v\)

\[
T(n) \leq T(n-1) + M(n)
\]

where \(M(n) = \) time to mult two \(n\) bit integers

\[
= \Theta(n^2 \log n \log \log n).
\]

**Fibonacci worst case:**

\[
u = F_k, \quad v = F_{k+1}
\]

where \(F_0 = 0, F_1 = 1, F_{k+2} = F_{k+1} + F_k, k \geq 0\)

\[
F_k = \frac{\Phi^k}{\sqrt{5}}, \quad \Phi = \frac{1}{2} \left(1 + \sqrt{5}\right)
\]

\[
\Rightarrow \text{Euclid's Algorithm takes } \log_\Phi \left(\sqrt{5} \cdot N\right) = \Theta(n)
\]

stages when \(N = \max(u, v)\).

**Improved Algorithm** (see AHU)

\[
T(n) \leq T\left(\frac{n}{2}\right) + O(M(n))
\]

\[
= \Theta(M(n) \log n)
\]

---

**Extended GCD Algorithm**

```
procedure ExGCD(u, v)

where \(u = (u_1, u_2, u_3)\), \(v = (v_1, v_2, v_3)\)

begin

if \(v_3 = 0\) then return(u)

else return ExGCD(v, u - \(\frac{v_1}{v_3} \cdot u_3\))
```

**Theorem**

\(\text{ExGCD((1,0,x),(0,1,y))}\)

\(=(x', y', \text{GCD}(x,y))\)

where \(x \cdot x' + y \cdot y' = \text{GCD}(x,y)\)

**Proof**

Inductively can verify on each call

\[
x_u + y_u = u_3
\]

\[
x_v + y_v = v_3
\]
Corollary

If $\gcd(x, y) = 1$ then $x'$ is the modular inverse of $x$ modulo $y$

proof

we must show $x \cdot x' = 1 \mod y$

but by previous Theorem,

$I = x \cdot x' + y \cdot y' = x \cdot x' \mod y$

so $I = x \cdot x' \mod y$

Gives Algorithm for Modular Inverse

Modular Laws for $n \geq 1$

let $x \equiv y$ if $x \equiv y \mod n$

Law A if $a \equiv b$ and $x \equiv y$ then $ax \equiv by$

Law B if $a \equiv b$ and $ax \equiv by$ and $\gcd(a, n) = 1$ then $x \equiv y$

let \( \{a_1, \ldots, a_k\} = \{b_1, \ldots, b_k\} \) if $a_i \equiv b_j$ for $i = 1, \ldots, k$ and $\{j_1, \ldots, j_k\} = \{1, \ldots, k\}$
**Fermat's Little Theorem**  
(proof by Euler)

If $n$ prime then $a^n = a \mod n$

**proof**

if $a = 0$ then $a^n = 0 = a$
else suppose $\gcd(a, n) = 1$

Then $x = ay$ for $y = a^{-1}x$ and any $x$
so $\{a, 2a, \ldots, (n-1)a\} = \{1, 2, \ldots, n-1\}$

So by Law A,

$$(a)(2a) \ldots (n-1)a = 1 \cdot 2 \cdot \ldots (n-1)$$

So $a^{n-1} = (n-1)! = (n-1)!$

So by Law B

$a^{n-1} = 1 \mod n$

$\varphi(n) = \text{number of integers in } \{1, \ldots, n-1\} \text{ relatively prime to } n$

**Euler's Theorem**

If $\gcd(a, n) = 1$

then $a^{\varphi(n)} = 1 \mod n$

**proof**

let $b_1, \ldots, b_{\varphi(n)}$ be the integers $< n$ relatively prime to $n$
\begin{lemma}
\{b_1, \ldots, b_{\phi(n)}\} \equiv \{ab_1, ab_2, \ldots, ab_{\phi(n)}\}
\end{lemma}

\textbf{proof}

If \(ab_i \equiv ab_j\) then by Law B, \(b_i \equiv b_j\)
Since \(1 = \gcd(b_i, n) = \gcd(a, n)\)
then \(\gcd(ab_i, n) = 1\) so \(ab_i = b_j\)
for \(\{j_1, \ldots, j_{\phi(n)}\} = \{1, \ldots, \phi(n)\}\)

By Law A and Lemma

\((ab_1)(ab_2) \cdots (ab_{\phi(n)}) \equiv b_1b_2 \cdots b_{\phi(n)}\)
so \(a^{\phi(n)} b_1 \cdots b_{\phi(n)} \equiv b_1 \cdots b_{\phi(n)}\)

By Law B \(a^{\phi(n)} \equiv 1 \pmod{n}\)

\begin{center}
\textbf{Taking Powers mod n by "Repeated Squaring"}
\end{center}

\textbf{Problem}

Compute \(a^e \pmod{b}\)

\(e = e_k e_{k-1} \cdots e_1 e_0\) \text{ binary representation}

\[1\] \(X \leftarrow 1\)
\[2\] \text{for } i = k, k-1, \ldots, 0 \text{ do }
\begin{align*}
\text{begin} \\
X &\leftarrow X^2 \pmod{b} \\
\text{if } &e_i = 1 \text{ then } X \leftarrow Xa \pmod{b} \\
\text{end}
\end{align*}

\text{output} \ \prod_{i=0}^{k} a^{e_i 2^i} = a^{\sum e_i 2^i} = a^e \pmod{b}

\textbf{Time Cost}

O(k) mults and additions mod b

\(k = \# \text{ bits of } e\)
Rivest, Sharmir, Adelman (RSA) Encryption Algorithm

**Method**

- Choose large random primes p, q
  - Let \( n = p \cdot q \)
- Choose large random integer \( d \)
  - Relatively prime to \( \varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1) \)
- Let \( e \) be the multiplicative inverse of \( d \) modulo \( \varphi(n) \)
  - \( e \cdot d \equiv 1 \mod \varphi(n) \)
  - (require \( e > \log n \), else try another \( d \))

**Cryptogram**

\[ C = E(M) = M^e \mod n \]

**Theorem**

If \( M \) is relatively prime to \( n \), and \( D(x) = x^d \mod n \) then

\[ D(E(M)) = E(D(M)) = M \]

**proof**

\[ D(E(M)) = E(D(M)) = M^{e \cdot d} \mod n \]

There must \( \exists \ k > 0 \) s.t.

\( 1 = \gcd(d, \varphi(n)) = -k \varphi(n) + de \)

So, \( M^{e \cdot d} = M^{k \varphi(n) + 1} \mod n \)

Since \( (p-1) \) divides \( \varphi(n) \)

\[ M^{k \varphi(n) + 1} = M \mod p \]

**By Euler's Theorem**

By Symmetry,

\[ M^{k \varphi(n) + 1} = M \mod q \]

Hence \( M^{e \cdot d} = M^{k \varphi(n) + 1} = M \mod n \)

So \( M^{ed} = M \mod n \)
Security of RSA Cryptosystem

Theorem
If can compute \( d \) in polynomial time, then can factor \( n \) in polynomial time

proof
\( e \cdot d - 1 \) is a multiple of \( \varphi(n) \)
But Miller has shown can factor \( n \) from any multiple of \( \varphi(n) \).

Corollary
If can find \( d' \) s.t.
\[ M^{d'} = M^d \mod n \]
\( \implies \) \( d' \) differs from \( d \) by \( \text{lcm}(p-1, q-1) \)
\( \implies \) so can factor \( n \).

Rabin's Public Key Crypto System

Use private large primes \( p, q \)

\begin{align*}
\text{public} & \quad n = q \cdot p \cdot \text{key} \\
\text{message} & \quad M \\
\text{cryptogram} & \quad M^2 \mod n
\end{align*}

Theorem
If cryptosystem can be broken, then can factor key \( n \)
proof

\[ \alpha = M^2 \mod n \text{ has solutions} \]
\[ M = \gamma, \beta, \ n-\gamma, \ n-\beta \]
where \( \beta \neq \{ \gamma, n-\gamma \} \)

But then \( \gamma^2 - \beta^2 = (\gamma - \beta)(\gamma + \beta) = 0 \mod n \)

So either (1) \( p | (\gamma - \beta) \) and \( q | (\gamma + \beta) \)

or either (2) \( q | (\gamma - \beta) \) and \( p | (\gamma + \beta) \)

In either case, two independent solutions for \( M \) give factorization of \( n \), i.e., a factor of \( n \) is \( \gcd(n, \gamma - \beta) \)

---

**Rabin's Algorithm**

for factoring \( n \), given a way to break his cryptosystem.

Choose random \( \beta \), \( 1 < \beta < n \) s.t. \( \gcd(\beta, n) = 1 \)

let \( \alpha = \beta^2 \mod n \)

find \( M \) s.t. \( M^2 = \alpha \mod n \)

by assumed way to break cryptosystem

\[ \text{With probability } \geq \frac{1}{2}, \]
\[ M \neq \{ \beta, n - \beta \} \]

\[ \Rightarrow \text{ so factors of } n \text{ are found} \]

\[ \text{else } \text{ repeat with another } \beta \]

**Note:** Expected number of rounds is 2
**Quadratic Residues**

\[ a \text{ is quadratic residue of } n \]
\[ \text{if } x^2 \equiv a \mod n \text{ has solution} \]

**Euler:**
- If \( n \) is odd, prime and \( \gcd(a, n) = 1 \), then
- \( a \) is quadratic residue of \( n \)
  - if \( a^{(n-1)/2} \equiv 1 \mod n \)

**Jacobi Function**

\[
J(a, n) = \begin{cases} 
1 & \text{if } \gcd(a, n) = 1 \text{ and } a \text{ is quadratic residue of } n \\
-1 & \text{if } \gcd(a, n) = 1 \text{ and } a \text{ is not quadratic residue of } n \\
0 & \text{if } \gcd(a, n) \neq 1 
\end{cases}
\]

**Gauss’s Quadratic Reciprocity Law**
- If \( p, q \) are odd primes,
- \( J(p, q) \cdot J(q, p) = (-1)^{(p-1)(q-1)/4} \)

**Rivest Algorithm:**

\[
J(a, n) = \begin{cases} 
1 & \text{if } a = 1 \\
J(a/2, n) \cdot (-1)^{(n^2-1)/8} & \text{if } a \text{ even} \\
J(n \mod a, a) \cdot (-1)^{(a-1)(n-1)/2} & \text{else} 
\end{cases}
\]
Theorem (Fermat)

\( n > 2 \) is prime iff

\[ \exists \ x, \ 1 < x < n \]

\( 1 \)

\( x^{n-1} \equiv 1 \mod n \)

\( 2 \)

\( x^i \neq 1 \mod n \) for all \( i \in \{1, 2, \ldots, n-2\} \)

---

Theorem & Primes NP

(Pratt)

**proof**

**input** \( n \)

\( n=2 \) \( \Rightarrow \) output "prime"

\( n=1 \) or \( n \) even and \( n>2 \) \( \Rightarrow \) output "composite"

**else** guess \( x \) to verify Fermat’s Theorem

Check (1) \( x^{n-1} \equiv 1 \mod n \)

To verify (2) guess prime factorization

\( \frac{n-1}{n_i} \)

\( (a) \) recursively verify each \( n_i \) prime

\( (b) \) verify \( x^{\frac{n-1}{n_i}} \neq 1 \mod n \)

**note**

if \( x^{\frac{n-1}{n_i}} = 1 \mod n \)

the least \( y \) s.t. \( x^y = 1 \mod n \) must divide \( n-1 \).

So \( x^a = 1 \mod n \)

let \( a = \frac{(n-1)}{n_i} \) so \( 1 \equiv x^a = x^{\frac{n-1}{n_i}} \mod n \)
**Primality Testing**

wish to test if n is prime

**technique**  
\[ W_n(a) = \begin{cases} 
\text{"a witnesses that } n \text{ is composite"} \\
\text{true} \Rightarrow n \text{ composite} \\
\text{false} \Rightarrow \text{don't know} 
\end{cases} \]

**Goal of Randomized Primality Tests:**

for random \( a \in \{1, \ldots, n-1\} \)  
\[ n \text{ composite } \Rightarrow \text{Prob}(W_n(a) \text{ true }) > \frac{1}{2} \]

So \( \frac{1}{2} \) of all \( a \in \{1, \ldots, n-1\} \)  
are "witnesses to compositness of n"

**Solovey & Strassen Primality Test**

\[ W_n(a) = (\gcd(a,n) \neq 1) \]

or \[ J(a,n) \neq a^{(n-1)/2} \mod n \]

test if Gauss's Quad. Recip. Law is violated
Definitions

\[ Z_n^* = \text{set of all nonnegative numbers } \leq n \]
which are relatively prime to \( n \).

**generator** \( g \) of \( Z_n^* \)
such that for all \( x \in Z_n^* \)
there is \( i \) such that \( g^i = x \mod n \)

*Theorem of Solovey & Strassen*

If \( n \) is composite, then \( |G| \leq \frac{n-1}{2} \)
where \( G = \{ a \mid W_n(a \mod n) \text{ false} \} \)

\[ \text{Case } G \neq Z_n^* \Rightarrow \text{G is subgroup of } Z_n^* \]
\[ \Rightarrow |G| \leq \frac{|Z_n^*|}{2} \leq \frac{n-1}{2} \]

**Case** \( G = Z_n \)
Use Proof by Contradiction

so \( a^{(n-1)/2} = J(a,n) \mod n \)
for all \( a \) relatively prime to \( n \)

Let \( n \) have prime factorization
\[ n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, \quad \alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_k \]

Let \( g \) be a generator of \( Z_{m_1}^* \) where \( m_1 = p_1^{\alpha_1} \)
Then by Chinese Remainder Theorem,

\[ \exists \text{unique } a \text{ s.t. } a = g \mod m \]

\[ a = 1 \mod \left( \frac{n}{m_i} \right) \]

Since \( a \) is relatively prime to \( n \),

\[ a \in \mathbb{Z}_n^* \text{ so } \]

\[ a^{\alpha_i - 1} = 1 \mod n \text{ and } g^{\alpha_i - 1} = 1 \mod n \]

Case \( \alpha_1 \geq 2 \).

Then order of \( g \) in \( \mathbb{Z}_n^* \)

\[ \alpha_i - 1 \]

is \( p_1 \) \((p_1 - 1)\) by known formula,

a contradiction since the order divides \( n-1 \).
We have shown $J(a,n) = -1 \mod n$
\[= -1 \mod \left( \frac{n}{m} \right)\]

But by assumption $a = 1 \mod \left( \frac{n}{m} \right)$

so $a^{(n-1)/2} = 1 \mod \left( \frac{n}{m} \right)$

Hence $a^{(n-1)/2} \neq J(a,n) \mod \left( \frac{n}{m} \right)$

*a contradiction with Gauss's Law!*

---

**Miller's Primality Test**

\[W_n(a) = \begin{cases} 
(gcd(a,n) \neq 1) \\
\text{or} \ (a^{n-1} \neq 1 \mod n) \\
\text{or} \ \gcd(a^{(n-1)/2^i} \mod n-1, n) \neq 1 \\
\text{for } i \in \{1, \ldots, k\} \\
\text{where } k = \max \{t \mid 2^t \text{ divides } n-1\}
\end{cases}\]

---

**Theorem**

(Miller)

*Assuming the extended RH, if* $n$ *is composite, then* $W_n(a)$ *holds for some* $a \in \{1, 2, \ldots, c \log^2 n\}$. 
Miller's Test assumes extended RH (not proved)

Rabin: choose a random \( a \in \{1, \ldots, n-1\} \) test \( W_n(a) \)

**Theorem** Rabin

if \( n \) is composite then

\[
\text{Prob} (W_n(a) \text{ holds}) > \frac{1}{2}
\]

⇒ gives another randomized, polytime algorithm for primality!