Algorithms
Professor John Reif

ALG 4.0

Number Theory Algorithms:

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

Main Reading Selections:
CLR, Chapter 33

Auxillary Reading Selections:
BB, Sections 8.5.2, 8.5.3, 8.6.2
Handout : "Lecture Notes on the Complexity of Some Problems in Number Theory"

Greatest Common Divisor

GCD(u,v) = largest a s.t.
a 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

$\Leftrightarrow$ a is a divisor of $u - \left(\lfloor u/v \rfloor\right) v$
$= u \bmod v$

Time Analysis of Euclid's Algorithm for n bit numbers u,v

$T(n) \le T(n-1) + M(n)$

$= O(n\, M(n))$

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

$= O(n^2 \log n \log\log n)$.

Fibonocci worst case:

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

where $F_0 = 0,\ F_1 = 1,\ F_{k+2} = F_{k+1} + F_k \ ,\ k \ge 0$

$$F_K = \frac{\Phi^k}{\sqrt{5}} \quad , \quad \Phi = \frac{1}{2}(1 + \sqrt{5})$$

$\Rightarrow$ Euclids Algorithm takes $\log_\Phi(\sqrt{5}\, N) = O(n)$ stages when $N = \max(u,v)$.

Improved Algorithm

(see AHU)

$$T(n) \le T\left(\frac{n}{2}\right) + O(M(n))$$

$$= O(M(n) \log n)$$

Extended GCD Algorithm

procedure $ExGCD(\vec{u}, \vec{v})$

where $\vec{u} = (u_1, u_2, u_3)$, $\vec{v} = (v_1, v_2, v_3)$

begin

if $v_3 = 0$ then return$(\vec{u})$

else return $ExGCD(\vec{v}, \vec{u} - (\vec{v} \lfloor u_3 / v_3 \rfloor))$

Theorem

$ExGCD((1,0,x),(0,1,y))$

$=(x', y', GCD(x,y))$

where $x x' + y y' = GCD(x,y)$

proof

inductively can verify on each call

$$\left(\begin{array}{l} x u_1 + y u_2 = u_3 \\ x v_1 + y v_2 = v_3 \end{array} \right.$$

Corollary

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

proof

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

but by previous Theorem,

$1 = x x' + y y' = x x' \bmod y$

so $1 = x x' \bmod y$

Gives Algorithm for *Modular Inverse* !

Modular Laws for $n \geq 1$

let $x \equiv y$ if $x = y \bmod n$

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 $\{a_1, \ldots, a_k\} \equiv \{b_1, \ldots, b_k\}$ if $a_i \equiv b_{j_i}$ 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 $a^n = a \bmod n$

proof

if $a \equiv 0$ then $a^n \equiv 0 \equiv a$

else suppose $\gcd(a,n) = 1$

Then $x \equiv ay$ for $y \equiv a^{-1}x$ and any x

so $\{a, 2a, \ldots, (n-1)a\} \equiv \{1, 2, \ldots, n-1\}$

So by Law A,

$$(a)(2a) \cdots (n-1)a \equiv 1 \cdot 2 \cdots (n-1)$$

$$\text{So } a^{n-1}(n-1)! \equiv (n-1)!$$

So by Law B

$$a^{n-1} \equiv 1 \bmod n$$

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

Euler's Theorem

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

then $a^{\varphi(n)} \equiv 1 \bmod n$

proof

let $b_1, \ldots, b_{\varphi(n)}$ be the integers < n relatively prime to n

Lemma

$\{b_1,\ldots, b_{\varphi(n)}\} \equiv \{ab_1, ab_2,\ldots,ab_{\varphi(n)}\}$

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 $ab_i = b_{j_i}$

for $\{j_1,\ldots, j_{\varphi(n)}\} = \{1,\ldots, \varphi(n)\}$

By Law A and Lemma

$$(ab_1)(ab_2)\cdots(ab_{\varphi(n)}) \equiv b_1 b_2 \cdots b_{\varphi(n)}$$

$$\text{so } a^{\varphi(n)} b_1 \cdots b_{\varphi(n)} \equiv b_1 \cdots b_{\varphi(n)}$$

By Law B $a^{\varphi(n)} \equiv 1 \mod n$

Taking Powers mod n **by "Repeated Squaring"**

Problem

Compute $a^e \mod b$

$e = e_k\, e_{k-1} \cdots e_1\, e_0$ binary representation

[1] $X \leftarrow 1$

[2] *for* $i = k, k-1,\ldots, 0$ *do*

begin

$X \leftarrow X^2 \mod b$

if $e_i = 1$ then $X \leftarrow Xa \mod b$

end

output $\prod_{i=0}^{k} a^{e_i 2^i} = a^{\Sigma e_i 2^i} = a^e \mod b$

Time Cost

O(k) mults and additions mod b

k = # bits of e

Rivest, Sharmir, Adelman(RSA) Encryption Algorithm

M = integer message

e = "encryption integer" for user A

Cryptogram

$$C = E(M) = M^e \bmod n$$

Method

(1) Choose large random primes p,q
let $n = p \cdot q$

(2) Choose large random integer d
relatively prime to $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$

(3) 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)

Theorem

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

$$D(E(M)) \equiv E(D(M)) \equiv M$$

proof

$$D(E(M)) \equiv E(D(M))$$
$$\equiv M^{e \cdot d} \mod n$$

There must $\exists\ k > 0$ s.t.

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

So, $M^{ed} \equiv M^{k\varphi(n)+1} \mod n$

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

$$M^{k\varphi(n)+1} \equiv M \mod p$$

By Euler's Theorem

By Symmetry,

$$M^{k\varphi(n)+1} \equiv M \pmod q$$

Hence $M^{ed} = M^{k\varphi(n)+1} = M \mod n$

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· d-1 is a multiple of φ(n)
But Miller has shown can factor n from any multiple of φ(n).

Corollary

If can find d' s.t.

$$M^{d'} = M^{d} \mod n$$

⇒ **d' differs from d by lcm(p-1, q-1)**

⇒ **so can factor n.**

Rabin's Public Key Crypto System

Use private large primes p,q

public **n = q p·** *key*

message **M**

cryptogram M^2 *mod n*

Theorem

If cryptosystem can be broken, then can *factor key n* *proof*

$\alpha = M^2 \bmod n$ 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) $p \mid (\gamma-\beta)$ and $q \mid (\gamma+\beta)$

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

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 β, $1 < \beta < n$ s.t. gcd(β,n)=1

let $\alpha = \beta^2 \mod n$

find M s.t. $M^2 = \alpha \bmod n$

by assumed way to break cryptosystem

With probability $\geq \frac{1}{2}$,

$M \neq \{\beta, \ n - \beta\}$

$\Rightarrow$ so factors of n are found

else repeat with another β

Note: Expected number of rounds is 2

Quadratic Residues

a is quadratic residue of n

if $x^2 \equiv a \mod n$ has solution

Euler:

If n is odd, prime and gcd(a,n)=1, then

a is quadratic residue of n

iff $a^{(n-1)/2} \equiv 1 \mod n$

Jacobi Function

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

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:

$$J(a,n) = \begin{cases} 1 & \text{if } a=1 \\ J(a/2,\, n) \cdot (-1)^{(n^2-1)/8} & \text{if } a \text{ even} \\ J(n \bmod a,\, a) \cdot (-1)^{\frac{(a-1)}{2}\frac{(n-1)}{2}} & \text{else} \end{cases}$$

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

$n=2 \implies$ output "prime"

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

else guess x to verify Fermat's Theorem

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

To verify (2) guess prime factorization

of $n-1 = n_1 \cdot n_2 \cdots n_k$

(a) recursively verify each n_i prime

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

note if $x^{(n-1)} = 1 \mod n$

the least y s.t. $x^{y} = 1 \mod n$ must divide $n-1$. So $x^{ya} = 1 \mod n$

let $a = \dfrac{(n-1)}{y n_i}$ so $1 \equiv x^{ya} = x^{(n-1)/n_i} \mod n$

Primality Testing

wish to test if n is prime

technique $W_n(a) =$ "*a witnesses that n is composite*"

$W_n(a) = \text{true} \Rightarrow$ n composite

$W_n(a) = \text{false} \Rightarrow$ don't know

Goal of Randomized Primality Tests:

for random $a \in \{1, \ldots, n-1\}$

n 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^* = set of all nonnegative numbers < 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 $G = \{a \mid W_n(a \bmod n) \text{ false}\}$

Case $G \neq Z_n^*$ $\Rightarrow$ 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

$n = P_1^{\alpha_1} P_2^{\alpha_2} \ldots P_k^{\alpha_k}$, $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_k$

Let g be a generator of $Z_{m_1}^*$ where $m_1 = P_1^{\alpha_1}$

Then by Chinese Remainder Theorem,

$\exists$ unique a s.t. $a = g \bmod m_1$

$a = 1 \bmod \left(\frac{n}{m_1}\right)$

Since a is relatively prime to n,

$a \in Z_n^*$ so

$a^{n-1} = 1 \bmod n$ and $g^{n-1} = 1 \bmod n$

Case $\alpha_1 \geq 2$.

Then order of g in Z_n^*

is $p_1^{\alpha_1 - 1}(p_1 - 1)$ by known formula,

a contradiction since the order divides n-1.

Case $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 1$

Since $n = p_1 \ldots p_k$

$$J(a,n) = \prod_{i=1}^{k} J(a, P_i)$$

$$= J(g, p_1) \cdot \prod_{i=2}^{k} J(1, p_i)$$

$$\text{since } a = \begin{cases} g \bmod p_i & i=1 \\ 1 \bmod p_i & i \neq 1 \end{cases}$$

So $J(a,n) = -1 \bmod n$

since $J(1, p_i) = 1$

and $J(g, p_1) = -1$

We have shown $J(a,n) = -1 \bmod n$

$$= -1 \bmod \left(\frac{n}{m_1}\right)$$

But by assumption $a = 1 \bmod \left(\frac{n}{m_1}\right)$

so $a^{(n-1)/2} = 1 \bmod \left(\frac{n}{m_1}\right)$

Hence $a^{(n-1)/2} \neq J(a,n) \bmod \left(\frac{n}{m_1}\right)$

a *contradiction with Gauss's Law!*

Miller's Primality Test

$W_n(a)$ = $(\gcd(a,n) \neq 1)$

or $(a^{n-1} \neq 1 \bmod n)$

or $\gcd(a^{(n-1)/2^i} \bmod n-1,\ n) \neq 1$

for $i \in \{1,\ldots,k\}$

where $k = \max\{i \mid 2^i \text{ divides } n-1\}$

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

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

$\Rightarrow$ **gives another randomized, polytime algorithm for primality!**