The RSA Cryptosystem: Primality Testing

Debdeep Mukhopadhyay

Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
INDIA -721302

Objectives

- **Quadratic Residues**
- **Primality Testing: Solovay Strassen Algorithm**
- **Computing the Jacobi Symbol**
- **Error bound for Solovay Strassen Algorithm**

The Quadratic Residue Problem

(Euler's Criterion) *Let p be an odd prime. Then a is a quadratic residue modulo p if and only if*

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

- **The time complexity of this check is $O(\log p)^3$ by applying square and multiply method to raise an element to a power.**
- **Note that if** $a^{(p-1)/2} \equiv -1 \pmod{p}$ **then a is a non-quadratic residue.**

Legendre Symbol

Suppose p is an odd prime. For any integer a, define the *Legendre symbol* $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Suppose p is an odd prime. Then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Jacobi Symbol

Suppose n is an odd positive integer, and the prime power factorization of n is

$$n = \prod_{i=1}^{k} p_i^{e_i}.$$

Let a be an integer. The *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined to be

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

Example

- **Compute** $\left(\frac{6278}{9975}\right)$
- **Note 9975=3x5^{2}x7x19**

$$\left(\frac{6278}{9975}\right) = \left(\frac{6278}{3}\right)\left(\frac{6278}{5}\right)^2\left(\frac{6278}{7}\right)\left(\frac{6278}{19}\right)$$

$$= \left(\frac{2}{3}\right)\left(\frac{3}{5}\right)^2\left(\frac{6}{7}\right)\left(\frac{8}{19}\right)$$

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

Prime vs Composite

- **Suppose n>1 is odd. If n is prime then**

$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} (\text{mod } n)$$

- **But if n is composite, it may or may not be the case that the above equation holds**
- **For any odd composite n, n is an Euler Pseudo-prime to the base a for at most half of the integers a Є Z_n^***

Error Probability of the algorithm

$$G(n) = \{a : a \in Z_n^*, \left(\frac{a}{n}\right) \equiv a^{(n-1)/2} (\text{mod } n)\}$$

First we shall prove that G(n) is a sub-group of Z_n^*. Hence, by Lagrange's Theorem, if

$$G(n) \neq Z_n^*, \text{ then } |G(n)| \leq \frac{|Z_n^*|}{2} \leq \frac{n-1}{2}$$

Suppose that $a, b \in G(n)$.

$$\therefore \left(\frac{a}{n}\right) \equiv a^{(n-1)/2} (\text{mod } n)$$

$$\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} (\text{mod } n)$$

Error Probability of the algorithm

It follows from the multiplicative rule of Jacobi symbols,

$$\left(\frac{ab}{n}\right) \equiv \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \equiv a^{(n-1)/2} b^{(n-1)/2} (\text{mod n}) \equiv (ab)^{(n-1)/2} (\text{mod n}).$$

$\therefore\ ab \in G(n).$

Since G(n) is a subset of a multiplicative finite group and is also closed under multiplication, then it must be a subgroup.

We next show that there exists at least an element in Z_n^* which does not belong to G(n).

Error Probability of the algorithm

Suppose, $n = p^k q,$ where p and q are odd, p is prime, $k \geq 2$, gcd(p,q)=1. Let, $a = 1 + p^{k-1}q.$

We have, $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)^k \left(\frac{a}{q}\right) = 1.$

Using Binomial theorem,

$$a^{(n-1)/2} = \sum_{i=0}^{(n-1)/2} \binom{(n-1)/2}{2} (p^{k-1}q)^i \equiv 1 + \frac{n-1}{2} p^{k-1} q (\text{mod n})$$

[as $k \geq 2$, the other terms in the Binomial expansion are 0 mod n]

Error Probability of the algorithm

If, $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} (\text{mod } n)$

$\Rightarrow \frac{n-1}{2} p^{k-1} q \equiv 0 (\text{mod n})$

$\Rightarrow p^k q \mid \frac{n-1}{2} p^{k-1} q \Rightarrow p \mid \frac{n-1}{2} \Rightarrow n \equiv 1 (\text{mod p}).$

But this contradicts the fact that $n \equiv 0 (\text{mod p})$.

Thus although $a \in Z_n^*$, it does not belong to G(n).

Thus, $|\text{G(n)}| \le \frac{n-1}{2}$.

Error Probability of the algorithm

Suppose, n is composite. If, $a \in Z_n \setminus Z_n^*$,

$\text{gcd(a,n)} \neq 1 \Rightarrow \left(\frac{a}{n}\right) \equiv 0$, thus algorithm gives always correct answer.

If, $a \in Z_n^*$, thus gcd(a,n) $\neq$ 1, Solovay Strassen returns wrong answer if and only if a $\in$ G(n). We proved that |G(n)| $\le$ (n-1)/2.

Thus, the probability of a wrong answer is:

$$\frac{|Z_n^*|}{n-1} \frac{|G(n)|}{|Z_n^*|} \le \frac{1}{2}$$

Example

- **91 is a pseudo prime number to the base 10**
- **Note that gcd(10,91)=1**

$$\left(\frac{10}{91}\right) \equiv 10^{(91-1)/2} (\text{mod } 91) \equiv 10^{45} (\text{mod } 91)$$

$$\equiv -1$$

- **If gcd(a,n)>1 then a and n have at least one common prime factor. Thus the Jacobi of a to the base n is 0. The condition is actually if and only if. Thus if Jacobi is 0 with respect to any a, n is composite. But remember the choice of a is random.**

Testing Primality

- **However if the Jacobi is not zero, then we check whether is is equal to a$^{(n-1)/2}$ mod n.**
- **If no, then it is composite.**
- **But if yes….**
  - **it can be prime**
  - **it can be pseudo-prime**
    - **we say it is prime**
    - **so the result can be erroneous**

Testing Primality

- **Luckily we have the following fact:**
  - **If the Jacobi is not zero wrt a then gcd(a,n)=1**
  - **So, $a \varepsilon Z_n^*$**
  - **For any odd composite n, n is an Euler pseudo-prime to the base a for at most half of the integers $a \varepsilon Z_n^*$**
  - **Thus we have the following Monte-Carlo Algorithm with error probability at most ½**

Solovay-Strassen Algorithm

SOLOVAY-STRASSEN(n)

choose a random integer a such that $1 \leq a \leq n-1$
$x \leftarrow \left(\frac{a}{n}\right)$
if $x = 0$
  then return ("n is composite")
$y \leftarrow a^{(n-1)/2} \pmod{n}$
if $x \equiv y \pmod{n}$
  then return ("n is prime")
  else return ("n is composite")

The decision problem is "Is n composite?".

Note that whenever the algorithm says "yes", the answer is correct.

Error may occur when the answer is "no" and the error probability is at most 1/2.

Rules to be remembered

1. If n is a positive odd integer and $m_1 \equiv m_2 \pmod{n}$, then

$$\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right).$$

2. If n is a positive odd integer, then

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{8} \\ -1 & \text{if } n \equiv \pm 3 \pmod{8}. \end{cases}$$

3. If n is a positive odd integer, then

$$\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right).$$

In particular, if $m = 2^k t$ and t is odd, then

$$\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^k \left(\frac{t}{n}\right).$$

4. Suppose m and n are positive odd integers. Then

$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{if } m \equiv n \equiv 3 \pmod{4} \\ \left(\frac{n}{m}\right) & \text{otherwise.} \end{cases}$$

An Example

$$\begin{aligned}
\left(\frac{7411}{9283}\right) &= -\left(\frac{9283}{7411}\right) && \text{by property 4} \\
&= -\left(\frac{1872}{7411}\right) && \text{by property 1} \\
&= -\left(\frac{2}{7411}\right)^4 \left(\frac{117}{7411}\right) && \text{by property 3} \\
&= -\left(\frac{117}{7411}\right) && \text{by property 2} \\
&= -\left(\frac{7411}{117}\right) && \text{by property 4} \\
&= -\left(\frac{40}{117}\right) && \text{by property 1} \\
&= -\left(\frac{2}{117}\right)^3 \left(\frac{5}{117}\right) && \text{by property 3} \\
&= \left(\frac{5}{117}\right) && \text{by property 2} \\
&= \left(\frac{117}{5}\right) && \text{by property 4} \\
&= \left(\frac{2}{5}\right) && \text{by property 1} \\
&= -1 && \text{by property 2.}
\end{aligned}$$

Computing Jacobi without factorization of n

- **Input: m≥0, n≥1, n odd**
- **Output: JacobiSymbol(m,n)**

```
if(m==0)
    { if(n==1) return 1; else return 0;}
else if (m>n)
    return JacobiSymbol(m mod n, n);
else{ m=2^δ m'; (where m'≥1, m' odd)
   return ±[JacobiSymbol(2,n)]^δ [JacobiSymbol(n,m')]
/* Use -, if m'≡n≡3 (mod n), + otherwise */}
```

Complexity

- **Roughly $O(\log n)^3$**
- **Only arithmetic operations are factoring out powers of two and modular reductions.**
- **Former depends on number of trailing zeros if the number is encoded as binary.**
- **So, dominated by modular reduction.**
- **Roughly O(log n) modular reductions necessary, each can be done in $O(\log n)^2$**

Repeated Application

- a: a random odd integer n of specified size is composite
- b: the algorithm answers n is prime m times in succession
- $Pr[b|a] \le 2^{-m}$, but we need $Pr[a|b]$.
- We apply Bayes' Theorem.

Repeated Application

- What is Pr[a]?
  - Assume $N \le n \le 2N$. Thus number of prime numbers between N and 2N is about:
    - $[2N/\ln(2N)]-[N/(\ln N)] \approx N/(\ln N) \approx n/\ln(n)$
    - Since there are $N/2 \approx n/2$ odd integers in this range, the probability of choosing a prime number is $2/\ln(n)$, and thus that of choosing composite number is:

$$Pr[a] \approx 1-[2/\ln(n)]$$

Repeated Applications

$$
\begin{aligned}
\mathbf{Pr}[\mathbf{a}|\mathbf{b}] &= \frac{\mathbf{Pr}[\mathbf{b}|\mathbf{a}]\mathbf{Pr}[\mathbf{a}]}{\mathbf{Pr}[\mathbf{b}]} \\
&= \frac{\mathbf{Pr}[\mathbf{b}|\mathbf{a}]\mathbf{Pr}[\mathbf{a}]}{\mathbf{Pr}[\mathbf{b}|\mathbf{a}]\mathbf{Pr}[\mathbf{a}] + \mathbf{Pr}[\mathbf{b}|\overline{\mathbf{a}}]\mathbf{Pr}[\overline{\mathbf{a}}]} \\
&\approx \frac{\mathbf{Pr}[\mathbf{b}|\mathbf{a}]\left(1 - \frac{2}{\ln n}\right)}{\mathbf{Pr}[\mathbf{b}|\mathbf{a}]\left(1 - \frac{2}{\ln n}\right) + \frac{2}{\ln n}} \\
&= \frac{\mathbf{Pr}[\mathbf{b}|\mathbf{a}](\ln n - 2)}{\mathbf{Pr}[\mathbf{b}|\mathbf{a}](\ln n - 2) + 2} \\
&\le \frac{2^{-m}(\ln n - 2)}{2^{-m}(\ln n - 2) + 2} \\
&= \frac{\ln n - 2}{\ln n - 2 + 2^{m+1}}.
\end{aligned}
$$

Error Probability of Solovay-Strassen

m	2^{-m}	bound on error probability
1	.500	.989
2	.250	.978
5	$.312 \times 10^{-1}$	.847
10	$.977 \times 10^{-3}$	.147
20	$.954 \times 10^{-6}$	$.168 \times 10^{-3}$
30	$.931 \times 10^{-9}$	$.164 \times 10^{-6}$
50	$.888 \times 10^{-15}$	$.157 \times 10^{-12}$
100	$.789 \times 10^{-30}$	$.139 \times 10^{-27}$

both becomes fairly small and negligible values and can be neglected.

References

- **D. Stinson, Cryptography: Theory and Practice, Chapman & Hall/CRC**

Next Days Topic

- **Factoring Algorithms**