Advanced Algorithms 28.2.2008, 3.3.2008,10.3.2008

Lecture Notes : Primality Testing

Professor: Naveen Garg *Scribes:Pushkar Tripathi and Amandeep Singh*

Introduction

In the previous lecture, we covered the Fermat's Primality test. In this lecture, we will look at Rabin Miller test, a more fullproof method of primality testing and analyse its effectiveness and running time. Before moving to the Rabin Miller test, let's review the Fermat's Test.

1 Fermat's Test

Theorem 1. ***Fermat's Little Theorem****: For a given number p,*

$$p \textit{ is Prime} \Rightarrow a^{p-1} = 1 mod\ p \qquad \forall a \in \{1, 2, \cdots p-1\}$$

Fermat's theorem follows from the fact that the group of integers modulo a prime p, form a group of size $p-1$ under multiplication. Let G be this group.Hence for any member(say a) of the group $a^{|G|} = 1$. Since $|G| = p-1$, this proves Fermat's Little Theorem.

1.1 Fermat's Primality testing Algorithm

In this section we will describe an algorithm based on fermat's test given in the previous section.

Input: A number n
Output: Prime or Composite

```
Choose random a $\in \{2 \cdots n\}$. Compute $a^{n-1}$ mod n
if $(a, n) \neq 1$ then
    return Composite
if $a^{n-1}$ mod n $\neq 1$, then
    return Composite
else
    return Prime
```

This algorithm returns **Prime** for all primes as proved by Fermat's Little Theorem. However, it may return **Prime** for some composite numbers too. Repeating this procedure whenever it returns **Prime** may help eliminate those errors which occurred due to the random choice of 'a'. However, there exist composite numbers for which this algorithm always returns **Prime**, irrespective of the choice of 'a'. Such numbers are called **Charmichael Numbers**.

Analysis of Fermat's Test

The following theorem states that at least half the numbers coprime to a non-charmichael number will give the correct certificate(of non-primality) if chosen in line 1 of the algorithm.

Theorem 2. *If n is not a Charmichael Number then atleast half the numbers coprime to n satisfy $a^{n-1} \neq 1$ mod n.*

Proof. This follows from the fact that numbers satisfying $(a, n) = 1$ mod n and $a^{n-1} = 1$ mod n form a subgroup of $\mathbf{Z}_n^*$. This is not a trivial subgroup since n is not a charmichael number. By langrange theorem the order of this subgroup must divide the order of the group $\mathbf{Z}_n^*$. Thus the size if the subgroup if atmost half the size of the group $\mathbf{Z}_n^*$. □

So for non-charmichael numbers the above algorithm is correct on for atleast half the choices of 'a'. Thus if it is repeated k times then the probability of declaring a composite number to be prime falls exponentially. This is summarized in the following two equations.

$$Pr\,[\text{n is decl. PRIME given n is composite, and non-charmichael}] \leq \frac{1}{2}$$

$$Pr\,[\text{n is decl. PRIME after k repetitions given n is composite and non-charmichael}] \leq (\frac{1}{2})^k$$

Hence the Fermat's algorithm works with good enough accuracy for Non Carmichael numbers.

2 Rabin-Miller Test

In the previous section, we analysed a randomized technique of primality testing that worked well for most numbers except for a small class of numbers. In this section we will analyse another randomized method that does not have such an achilles' heal. This primality test relies on finding the square roots of unity in the group $\mathbf{Z}_n^*$. In the next few lines we will define the square-roots of unity and explore their properties.
Square root of unity: In a group G, the square root of unity is an element $x \in$ G, such that $x^2 = 1$.

Theorem 3. *For a given prime, p, there are exactly two square roots of unity in the group $\mathbf{Z}_p^*$. These are the trivial roots ± 1.*

Proof. Let x($\leq p$) be a root of unity, then the following equations follow.

$$\begin{aligned} x^2 &\equiv 1 \qquad \textit{mod } p \\ x^2 - 1 &\equiv 0 \qquad \textit{mod } p \\ (x-1)(x+1) &\equiv 0 \qquad \textit{mod } p \end{aligned}$$

Thus p divides either $x - 1$ or $x + 1$. But x is no greater than p, thus x equals ± 1. □

Before we continue further let us recall the Chinese Remainder Theorem.

Theorem 4. ***Chinese Remainder Theorem :*** *If p and q be two positive integers such that $(p, q) = 1$ then the following set of equations have a unique solution modulo pq.*

$$\begin{aligned} x &\equiv a \ (mod \ p) \\ x &\equiv b \ (mod \ q) \end{aligned}$$

Theorem 5. *For any composite number n, there are atleast two non-trivial square roots of unity in the group $\boldsymbol{Z}_n^*$.*

Proof. Proof follows from induction on the number n. We can see that the base case for $n = 2$ is trivially true. Assume that the theorem holds for all $k < n$. Let $n = ab$ such that $(a, b) = 1$. Then by chinese remainder theorem the following equations have a unique solution mod n.

$$y \equiv 1 \ (mod \ a) \tag{1}$$

$$y \equiv -1 \ (mod \ b) \tag{2}$$

Clearly y$\neq \pm 1$ and also the following two relations hold for y^2.

$$y^2 \equiv 1 \ (mod \ a) \tag{3}$$

$$y^2 \equiv 1 \ (mod \ b) \tag{4}$$

Using the fact that $(a, b) = 1$ and equations (3) and (4) the solution to equations (1) and (2) gives a non trivial square root of unity mod n. □

These theorems collectively prove that if the given number n is prime iff it there are exactly two trivial square-roots of unity mod n.

Rabin Miller Primality Testing Algorithm

We can safely say that the candidate number(say n) is odd hence, $n - 1$ is even. Let

$$n - 1 = 2^t s, \text{ s is odd}$$

Construct the following sequence for $\alpha \in \mathbf{Z}_n^*$ by repeatedly squaring α^s .

$$S_\alpha = \left\{ S_\alpha(i) = \alpha^{2^i s} \ (mod \ n) \mid i \in \{0, 1, 2, 3 \cdots t\} \right\}$$

If the last element in this sequence is not 1, then n is surely composite. If the 1^{st} element of the sequence is 1, we declare n to be prime. Let k be the smallest index at which $S_\alpha(k) = 1$ is such that $S_\alpha(k - 1) \neq -1$, then we have found a non-trivial square root of unity and hence a certificate of the compositeness of n.

However, if $S_\alpha(k - 1) = -1$, then we cannot be sure about the primality of n. As in the previous algorithm, we want an upper bound on the probability of n being composite when such a certificate cannot be produced for the random choice of α.

Analysis of the Rabin Miller method

To analyze the effectiveness of the procedure for random choice of α we will prove that the set of bad choices of α (ones that donot give a certificate of compositeness) is contained in a non-trivial subgroup of Z_n^*. Theorem 6 proves that this subgroup is not empty while proposition 7 will prove that all such α lie in this subgroup.

Define $\alpha \in \mathbf{Z}_n^*$ to be a **witness** if by choosing it as the starting number in the procedure described above we would have arrived at a certificate of the compositeness of n. Similarly define **non-witnesses** in Z_n^* .

Define k as follows,

$$k = \max_{i \in \{0,1,2 \cdots \phi(n)\}} \left\{ j \mid \alpha_i^{2^j s} \equiv -1 \quad mod \quad n \right\}$$

Note that $n-1 \in \mathbf{Z}_n^*$. Since $n-1 \equiv -1$ mod n and s is odd, $(n-1)^s \equiv -1$ mod n. So, there surely exists an element α of $\mathbf{Z}_n^*$ such that $-1 \in S_\alpha$ and hence k always exists.

Theorem 6. *If n is composite then there exists an $\alpha \in \boldsymbol{Z}_n^*$ such that α is a witness.*

Proof. **Case 1: n = ab and (a,b) = 1. i.e. n is not a prime power.**

Pick any row(say corresponding to v) such that $v^{2^k s} \equiv -1$ (mod n). Define w as follows,

$$\begin{aligned} w &\equiv v \ (mod\ a) \quad (5) \\ w &\equiv 1 \ (mod\ b) \quad (6) \end{aligned}$$

By Chinese remainder theorem there exists a **unique w** which satisfies equations 5 and 6. The following propositions complete the proof for this case.

Proposition 7. *For the variable w defined above, $w^{2^k s} \neq \pm 1$(mod n) but $w \in \boldsymbol{Z}_n^*$.*

Proof. Let $w^{2^k s} \equiv 1$(mod n). This implies $w^{2^k s} \equiv 1$(mod a). By equation 5 and using our assumption it follows that,

$$\begin{aligned} w &\equiv v \ (mod\ a) \\ w^{2^k s} &\equiv v^{2^k s} \ (mod\ a) \\ w^{2^k s} &\equiv -1 \ (mod\ a) \end{aligned}$$

This contradicts our assumption.
On the other hand if we assume $w^{2^k s} \equiv -1$(mod n) then $w^{2^k s} \equiv 1$(mod b).By equation 6 and using our assumption it follows that,

$$\begin{aligned} w &\equiv 1 \ (mod\ b) \\ w^{2^k s} &\equiv 1^{2^k s} \ (mod\ b) \\ w^{2^k s} &\equiv 1 \ (mod\ b) \end{aligned}$$

This contradicts our assumption.

□

Hence w$^{2^k s} \neq \pm 1$(mod n). But by the given equations 5 and 6, $(w, a) = (w, b) = 1$. Since w and a have no common factor and neither do w and b and a and b are co-prime. w and ab have no commen factor. Thus, $(w, ab) = 1$, i.e. w $\in \mathbf{Z}_n^*$.

Case 2: n = p^r i.e. n is the power of a prime
It was discussed in class that the following procedure be invoked at the beginning of our algorithm to check for this case and hence to issue a compositeness-certificate to n.

Input: A number, n
Output: true if n is the power of a number else false.

```
for all $k \in \{1, 2 \cdots log_2(n)\}$ do
    Binary search for r such that r$^k = n$
    if $\exists$ r such that r$^k = n$ then
        return Power of Prime
return Not the Power of Prime
```

This gives a computational(O(log$_2^3$(n)) procedure) way to eleminate the this case in the beginning of the algorithm. We can also handle this case analytically. For this we will use the following theorem (without proof).

Theorem 8. *$\mathbf{Z}_n^*$ is a cyclic group.*

Let g be the generator for $\mathbf{Z}_n^*$. Thus $\phi(n)$ is the least number such that

$$g^{\phi(n)} \equiv 1 \ (mod \ n)$$

Proposition 9. *n is not a Charmichael number.*

Proof. We need to find a number r, such that r and n are coprime and $r^{n-1} \neq 1$ (mod n). If possible let g(as defined earlier) be such that $g^{n-1} \equiv 1$ (mod n). Then $\phi(n)$ divides n-1. This means $p^r - p^{r-1}$ divides $p^r - 1$ which is not possible. Hence there exists a number(g) for which $g^{n-1} \neq 1$ (mod n). Thus n is not a charmicheal number. □

□

Theorem 10. *Atleast half the elements of $\mathbf{Z}_n^*$ are witnesses.*

Proof. Define the set B as follows,

$$B = \left\{ a \in \mathbf{Z}_n^* \mid a^{2^k s} \equiv \pm 1(\text{mod n}) \right\}$$

We can easily see that each non-witness lies in B. B may contain some witnesses. We can also see that B is a subgroup of $\mathbf{Z}_n^*$. So if we can prove that it is a non-trivial subgroup then its order must divide that of $\mathbf{Z}_n^*$. Hence order of B will be at most half the size of $\mathbf{Z}_n^*$. □

Theorem 11. *For any arbitrary composite number n, the event that for a random choice of α we are unable to issue a certificate of compositeness happens with probability less than $\frac{1}{2}$.*

Proof. The proof follows from the theorems given above. □

By repeating the above procedure k times we can boost the probability of issuing correct-certificates to all numbers. Note that the Rabin-Miller test does not suffer from the problems of Fermat's test. Unlike the Fermat's test **there is no bad input for Rabin-Miller test**.