COM 5335 NETWORK SECURITY LECTURE 8 PRIMALITY TESTING

Scott CH Huang

Definition

- A prime number is a positive integer p having exactly two positive divisors, 1 and p.
- A composite number is a positive integer $n > 1$ which is not prime.

Primality Test vs Factorization

- Factorization's outputs are non-trivial divisors.
- Primality test's output is binary: either PRIME or COMPOSITE

Naïve Primality Test

- Input: Integer n > 2
- Output: PRIME or COMPOSITE

```
for (i from 2 to n-1){
        if (i divides n)
                return COMPOSITE;
}
return PRIME;
```

Still Naïve Primality Test

- Input/Output: same as the naïve test

```
for (i from 2 to √n ){
        if (i divides n)
                return COMPOSITE;
}
return PRIME;
```

Sieve of Eratosthenes

- Input/Output: same as the naïve test

Let A be an arry of length n

Set all but the first element of A to TRUE

for (i from 2 to $\sqrt{n}$){

    if (A[i]=TRUE)

        Set all multiples of i to FALSE

}

if (A[i]=TRUE) return PRIME

else return COMPOSITE

Primality Testing

- Two categories of primality tests
- Probablistic
  - *Miller-Rabin Probabilistic Primality Test*
  - *Cyclotomic Probabilistic Primality Test*
  - *Elliptic Curve Probabilistic Primality Test*
- Deterministic
  - *Miller-Rabin Deterministic Primality Test*
  - *Cyclotomic Deterministic Primality Test*
  - *Agrawal-Kayal-Saxena (AKS) Primality Test*

Running Time of Primality Tests

- Miller-Rabin Primality Test
  - *Polynomial Time*
- Cyclotomic Primality Test
  - *Exponential Time, but almost poly-time*
- Elliptic Curve Primality Test
  - *Don’t know. Hard to Estimate, but looks like poly-time.*
- AKS Primality Test
  - *Poly-time, but only asymptotically good.*

Fermat’s Primality Test

- It’s more of a “compositeness test” than a primality test.
- Fermat’s Little Theorem:

  If *p* is prime and $a \nmid p$, then $a^{p-1} \equiv 1 \pmod{p}$
- If we can find an *a* s.t. $\gcd(a, n-1) = 1, a^{n-1} \not\equiv 1 \pmod{n}$

  , then *n* must be a composite.
- If, for some *a*, *n* passes the test, we cannot conclude *n* is prime. Such n is a *pseudoprime*. If this pseudoprime *n* is not prime, then this *a* is called a **Fermat liar.**
- If, for all $1 \leq a \leq n-1, s.t.\ \gcd(a, n-1) = 1$

  we have $a^{n-1} \not\equiv 1 \pmod{n}$ can we conclude *n* is prime?
- No. Such *n* is called a **Carmichael number.**

Some Small Carmichael Numbers

Carmichael Numbers	Corresponding Factorizations
561	3*11*17
41041	7*11*13*14
825265	5*7*17*19*73
321197185	5*19*23*29*37*137

Carmichael numbers < 100,000
561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, and 75361.

Pseudocode of Fermat's Primality Test

FERMAT(*n*,*t*){

INPUT: odd integer $n \geq 3$, # of repetition *t*

OUTPUT: PRIME or COMPOSITE

```
    for (i from 1 to t){
        Choose a random integer a s.t. 2 ≤ a ≤ n-2
        Compute r ≡ a^(n-1) (mod n)
        if ( r ≠ 1 )    return COMPOSITE
    }
    return PRIME
}
```

Where: Compute $r \equiv a^{n-1} \pmod{n}$; if ($r \neq 1$) **return** COMPOSITE

Miller-Rabin Probabilistic Primality Test

- It’s more of a “compositeness test” than a primality test.
- It does not give proof that a number n is prime, it only tells us that, with high probability, n is prime.
- It’s a randomized algorithm of Las Vegas type.

A Motivating Observation

FACT:

Let p be an odd prime. $x \in \mathbb{Z}_p^*$. If $x^2 = 1$ then $x = \pm 1$

Moreover, if $n - 1 = m2^k$, and m is odd.

Let $a \in \mathbb{N}, s.t.\ \gcd(a, n) = 1$. Then either

$a^m \equiv 1 \pmod{n}$ or $a^{m2^i} \equiv -1 \pmod{n}$ for some

$0 \leq i \leq k - 1$

Miller-Rabin Algorithm

- If $a^m \not\equiv 1$ and $a^{m2^i} \not\equiv -1 \pmod{n}, \forall\, 0 \leq i \leq k-1$

  Then a is a strong witness for the compositeness of n.

- If $a^m \equiv 1 \pmod{n}$ or $a^{m2^i} \equiv -1 \pmod{n}$ for some $0 \leq i \leq k-1$ *then n is called a pseudoprime w.r.t. base a, and a is called a strong liar.*

Miller-Rabin: Algorithm Pseudocode

```
MILLER-RABIN(n,t){
INPUT: odd integer n ≥ 3, # of repetition t
    Compute k & odd m s.t. n − 1 = m2^k
    for ( j from 1 to t ){
        Choose a random integer a s.t. 2 ≤ a ≤ n − 2
        Compute y ≡ a^m (mod n)
        if ( y ≠ 1 and y ≠ n − 1 ){
            Set i ← 1
            while( i ≤ k − 1 and y ≠ n − 1 ){
                Set y ← y^2 (mod n)
                if ( y = 1 ) return COMPOSITE
                else i ← i + 1
            }
            if ( y ≠ n − 1 ) return COMPOSITE
        }
    }
    return PRIME
}
```

Miller-Rabin: Example

- n = 2465=5*17*29 (a Carmichael number)
- n-1=2464=2^5*7*11
- a^{m2^i} values shown as below

	i=5	4	3	2	1	0
a=2	1	1	1	1886	1449	1902
a=3	1	1	1886	1016	144	2018
a=5	1480	1480	900	30	1335	2145
a=7	1	1	1886	871	784	2437
a=11	1	1	1886	871	1681	1061
a=13	1	1	1	1	2379	608
a=47	1	1	1	1	-1	302

Miller-Rabin: Main Theorem

- Theorem:

  Given $n > 9$. Let B be the number of strong liars. Then

$$\frac{B}{\varphi(n)} \leq \frac{1}{4}$$

- If the Generalized Riemann Hypothesis is true, then
- Miller-Rabin primality test can be made deterministic by running MILLER-RABIN(n, $2\log^2 n$)