Primality Testing

Christophe Clavier

University of Limoges

Master 2 Cryptis

Introduction

A primality test is a test which determines whether an integer is prime or composite.

This is not the same problem as decomposing an integer into the product of its prime factors (factorization problem).

There are two families of primality tests:

- Provable primality tests (deterministic) which determine the primality with certainty.
- Probabilistic primality tests for which there is a (negligeable) probability that a composite integer is declared prime.

Generalities

- A provable primality test is deterministic.
- When declaring an integer n as being prime, it is mathematicaly proven that n is prime.
- Some provable primality tests are also able to produce a small piece of data (a certificate) from which it is fast to verify that the primality proof is correct.
- The major drawback of these tests is their (relative) inefficiency.

General Usage Primality Tests

- Elliptic Curve Primality Proving (ECPP)
  - Atkin's method (1986) has been implemented by François Morain and gives the method of choice for proving the primality of general integer.
  - In April 2011, this implementation proved the primality of a 26 643 digits general integer.
    (http://www.lix.polytechnique.fr/Labo/Francois.Morain/Primes/myprimes.html)
- AKS, the only one known polynomial-time provable primality test
  - In 2002, Agrawal, Kayal & Saxena created a big surprise by proving the conjecture that *PRIMES* is in *P*.
  - Their method allowed to prove the primality of any integer n with asymptotic complexity $\mathcal{O}(\log^{12} n)$. (now $\mathcal{O}(\log^{10.5} n)$)

Dedicated Usage Primality Tests

There exist numerous tests (based on the factorization of $n-1$ or $n+1$) which allow to efficiently prove the primality of special kinds of integers:

- The Lucas-Lehmer test for Mersenne numbers ($M_p = 2^p - 1$)
  - Considering the recurence $s_n \equiv s_{n-1}^2 - 2 \pmod{M_p}$, and $s_0 \equiv 4$, the Mersenne number M_p is prime if and only if $s_{p-2} \equiv 0 \pmod{M_p}$.
  - On January 7, 2016, was found the 49$^{\text{th}}$ known Mersenne prime $M_{74\,207\,281} = 2^{74\,207\,281} - 1$ (22 338 618 decimal digits). (http://www.mersenne.org)
- The Pepin test for Fermat numbers ($F_n = 2^{2^n} + 1$)
  - Fermat number F_n is prime if and only if $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.
- The Proth test which is a generalization of the Pepin test
  - Allows to prove the primality of $n = hq^k + 1$, with q prime and $q^k > h$.
- ...

General Principle

A probabilistic primality test is essentialy a procedure which inputs an integer, and outputs one of the following answers:

- This integer is composite.
- *I found no reason why this integer should not be prime.*

General Principle

For each odd integer n, a probabilistic primality test defines a set $\mathcal{W}(n) \subset \mathbb{Z}_n$ with the following properties:

(i) Given $a \in \mathbb{Z}_n$, it is possible to test in polynomial time whether $a \in \mathcal{W}(n)$

(ii) If n is prime, then $\mathcal{W}(n) = \varnothing$

(iii) If n is composite, then $|\mathcal{W}(n)| \geqslant \frac{n}{2}$ (except for possibly rare exceptions)

Definition

If n is composite, then:

- elements from $\mathcal{W}(n)$ are called witnesses (of the compositeness of n),
- elements from $\mathcal{L}(n) = \mathbb{Z}_n \backslash \mathcal{W}(n)$ are called liars.

How does it work ?

One have to test the integer n for primality.

One picks a at random in $\mathbb{Z}_n$ (a is called the base), and one tests whether $a \in \mathcal{W}(n)$.

If $a \in \mathcal{W}(n)$ the test answers composite:

- n fails to the primility test with base a.
- n is then proven to be composite.

If $a \notin \mathcal{W}(n)$ the test answers *prime*:

- n passes to the primility test with base a.
- n is only presumed to be prime.

Strictly speaking, this is a compositeness test, rather than a primality test.

How does it work ?

A single application of the test answering composite is enough to know for sure that n is composite.

Successive and independant applications of the test, each answering *prime*, lead to increasing confidence in the primality of n.

One can reach an arbitrarily large level of confidence:

- If the test is applied independantly t times on a composite integer n, the probability that n is declared *prime* for each one of the bases, is upper bounded by $(\frac{1}{2})^t$.

Definition

A probable prime is an integer n which is presumed to be prime, based on a probabilistic primality test.

Definition

A base a pseudoprime is a composite integer n which passes the primality test with the base a.

Fermat Test

Fermat's Theorem

Theorem (Fermat's little theorem)

For any prime p,

$$\gcd(a,p) = 1 \quad \Rightarrow \quad a^{p-1} \equiv 1 \pmod{p}$$

$$\left[\Rightarrow \forall a,\ 1 \leqslant a \leqslant p-1, \quad a^{p-1} \equiv 1 \pmod{p}\right]$$

Université de Limoges

Fermat Test

Fermat witness, liar, pseudoprime

Definition

One defines $\mathcal{W}(n)$ as:
$\mathcal{W}(n) = \{a \in \mathbb{Z}_n \text{ such that } a^{n-1} \not\equiv 1 \pmod{n}\}$

Definition

Let n be an odd composite integer.
An integer a, $1 \leqslant a \leqslant n-1$, such that $a^{n-1} \not\equiv 1 \pmod{n}$ is called a Fermat witness of compositeness for n.

Definition

Let n be an odd composite integer.
An integer a, $1 \leqslant a \leqslant n-1$, such that $a^{n-1} \equiv 1 \pmod{n}$ is called a Fermat liar for n.
n is then called a base a Fermat pseudoprime.

Fermat Test

Example

Example

$n = 341 = 31 \cdot 11$ is a Fermat base 2 pseudoprime, since $2^{340} \equiv 1 \pmod{341}$

Proof.

$$\begin{aligned} 2^{340} &= (2^{10})^{34} \\ &\equiv 1^{34} \pmod{341} \end{aligned}$$

$\square$

Fermat Test

Algorithm

Algorithm 1 Fermat Primality Test

Input: An odd integer $n \geqslant 3$, and a security parameter $t \geqslant 1$
Output: An answer to the question whether n is composite or *prime*

```
procedure FERMAT(n, t)
    for i from 1 to t do
        Pick an integer a at random in [2, n − 2]
        Compute y = a^(n−1) mod n
        if y ≠ 1 then
            return composite
        end if
    end for
    return prime
end procedure
```


When Fermat algorithm returns *prime*, there is no certainty that n is indeed prime, but ...

...it is known that pseudoprimes for a given base a are quite rare.

So Fermat test provide a correct answer for almost all inputs.

WARNING: This does not mean that Fermat test provides a correct answer with almost all bases, for any input !

Indeed, there exist (rare) composite integers which are declared *prime* with almost any base !

Definition

A Carmichael number is a composite n which is pseudoprime with any base a verifying $\gcd(a, n) = 1$. (Example: $n = 561$)

- It is quasi impossible to identify a Carmichael number as composite by means of Fermat test.
- The test will succeed on Carmichael numbers (answering composite) only for bases a such that $\gcd(a, n) > 1$.

  (This is quite rare if n has been checked for divisibility by small primes.)

Theorem

A composite integer n is a Carmichael number if and only if:

(i) *n is square free,*

(ii) *$(p-1) \mid (n-1)$ for all prime p dividing n.*

- In 1994, Alford, Granville and Pomerance proved that there exist infinitely many Carmichael numbers. (Fortunately they are quite rare.)

Theorem (Miller-Rabin criterion)

Let p be a odd prime integer ($p - 1 = 2^s r$, with r odd).
Let a be an integer verifying $\gcd(a, p) = 1$.

Then, one of the following conditions holds:

(i) $a^r \equiv 1 \pmod{p}$

(ii) $\exists\, j,\ 0 \leqslant j \leqslant s-1,$ *such that* $a^{2^j r} \equiv -1 \pmod{p}$

Example

$p = 97 \qquad p - 1 = 2^5 \cdot 3$

a	a^3 mod 97	a^6 mod 97	a^{12} mod 97	a^{24} mod 97	a^{48} mod 97
2	8	64	22	96	1
4	64	22	96	1	1
5	28	8	64	22	96
6	22	96	1	1	1
35	1	1	1	1	1
36	96	1	1	1	1

Definition

Let n be an odd composite integer ($n-1 = 2^s r$, with r odd), and a base a, $1 \leqslant a \leqslant n-1$,

- if the Miller-Rabin criterion is not verified for n with base a,
  ($a^r \not\equiv 1 \pmod{n}$ and $a^{2^j r} \not\equiv -1 \pmod{n}\ \forall\, 0 \leqslant j \leqslant s-1$)
  then the base a is called a strong witness of compositeness for n,
- if the Miller-Rabin criterion is verified for n with base a,
  ($a^r \equiv 1 \pmod{n}$ or $\exists\, 0 \leqslant j \leqslant s-1$ such that $a^{2^j r} \equiv -1 \pmod{n}$)
  then a is called a strong liar for n, and n is a base a strong pseudoprime.
  (n behaves as a prime when verifying the Miller-Rabin criterion for the base a.)

Example

$n = 91 = 7 \cdot 13$

- $15^{45} \equiv 57 \pmod{91}$, so 15 is a strong witness proving 91 is composite.
- $9^{45} \equiv 1 \pmod{91}$, so 9 is a strong liar for 91 (a base 9 strong pseudoprime).

Algorithm 2 Miller-Rabin Primality Test

Input: An odd integer $n \geqslant 3$, and a security parameter $t \geqslant 1$
Output: An answer to the question whether n is composite or *prime*

```
procedure MILLER-RABIN(n, t)
    Write n − 1 as 2^s · r, with r odd
    for i from 1 to t do
        Pick an integer a at random in [2, n − 2]
        y ← a^r mod n
        if y ≠ 1 and y ≠ n − 1 then
            j ← 1
            while j ⩽ s − 1 and y ≠ n − 1 do
                y ← y^2 mod n
                if y = 1 then return composite
                end if
                j ← j + 1
            end while
            if y ≠ n − 1 then return composite
            end if
        end if
    end for
    return prime
end procedure
```

Theorem

If n is an odd composite integer, then at most $\frac{1}{4}$ of all bases $1 \leqslant a \leqslant n-1$ are strong liars for n.

Furthermore, if $n \neq 9$ then the number of strong liars for n is at most $\frac{\varphi(n)}{4}$.

$\Rightarrow$ *For any odd composite integer n, the probabiliy that n is declared prime after t iterations of the Miller-Rabin test is less than $\left(\frac{1}{4}\right)^t$.*

- For almost every composite integer n, the number of strong liars for n is actualy much less than the upper bound $\frac{\varphi(n)}{4}$.
- The error probability of the Miller-Rabin test is much less than $\left(\frac{1}{4}\right)^t$ for almost any n.

Example

- $105 = 3 \cdot 5 \cdot 7$ has only 2 strong liars (1 and 104).
- The smallest base 2 strong pseudoprime is 2 047.
- The smallest base 2 and base 3 strong pseudoprime is 1 373 653.

Comparison between Fermat and Miller-Rabin tests

- Any strong liars for n is also a Fermat liar for n.
- $\Rightarrow$ Any pseudoprime for Miller-Rabin test is also a pseudoprime for Fermat test.
- There is no recalcitrant composite for Miller-Rabin test (like Carmichael numbers for Fermat test).
- Miller-Rabin test needs (few) less modular multiplications than Fermat test.
- The upper bound for the error probability is lower for Miller-Rabin test than for Fermat test.

There is no good reason to prefer Fermat test to Miller-Rabin test

Université de Limoges