CS810A/MA810A Computer Algebra

Alex Myasnikov and Werner Backes

Stevens Institute of Technology

CS810A/MA810A 2008
Primality testing.

- In practice often need to deal with large primes.
- It happens that prime numbers are not too rare.
- Still need to decide whether a number is prime or not - primality testing.
Primality testing.

- Naive tests (factorization)
- Probabilistic tests:
  - Fast and simple
  - Have small probability of error.
- Deterministic tests (Agrawal, Saxena, Kayal $O((\log n)^6)$):
  - Slower than probabilistic
  - Difficult and therefore prune to programming errors.
Primality testing: pseudoprimes.

- Recall by Fermat’s theorem $a^{p-1} = 1 \mod p$ for all $a \in \mathbb{Z}_p$, when $p$ is prime.
- If for a given $n$ there exists $a$ s.t. $a^{n-1} \neq 1 \mod n$ then $a$ is a “witness” that $n$ is not a prime.

**Definition (Pseudoprime)**

A composite integer $n \in \mathbb{Z}^+$ is called a base-$a$ pseudoprime if

$$a^{n-1} = 1 \mod n.$$ 

We will deal with odd numbers only.
**PROCEDURE**  Fermat’s test

**INPUT:**  Odd $n \in \mathbb{Z}^+$

**OUTPUT:**  COMPOSITE or PROBABLY PRIME

1:  **IF** $2^{n-1} \neq 1 \mod n$ **THEN**

2:  **RETURN** COMPOSITE

3:  **ELSE**

4:  **RETURN** PROBABLY PRIME
Primality testing: Fermat’s test.

- Fermat’s test is correct when returns COMPOSITE (2 is a witness)
- We do not know for sure otherwise
- What is the error probability of the Fermat’s test?
Primality testing: Fermat’s test.

- Only 22 values of $n < 10000$ when test errors
- One in a million chance of a 50-bit random number being base-2 pseudoprime.

Problem: there are numbers for which test fails with any base $a$
Definition (Carmichael numbers)
A composite positive integer \( n \) is called a Carmichael number if

\[ a^{n-1} \equiv 1 \pmod{n} \]

for all \( a \) such that \( \gcd(a, n) = 1 \).

- Carmichael numbers are rare: there are only 2,163 of them less than 25,000,000,000.
If $p$ is an odd prime, then the equation

$$x^2 = 1 \mod p$$

has only two solutions: $x = 1$ and $x = -1$.

- **Corollary:** if there exists a nontrivial square root of 1 modulo $n$, then $n$ is composite.
- We can use this and incorporate the check when computing modulo exponentiation.
- Does not depend on $n$
Miller-Rabin test:
- Test several, randomly chosen bases \( a \)
- Test if nontrivial square roots of 1 ever discovered during exponentiation.
Primality testing: Miller-Rabin test.

**PROCEDURE**  Witness

**INPUT:**  Odd \( n \in \mathbb{Z}^+ \), \( a \in MZ_n \)

**OUTPUT:**  TRUE if \( a \) is a witness of compositeness of \( n \)

1:  LET \(< b_k, \ldots, 1 >\) be binary of \( n - 1 \) and \( d = 1 \)

2:  FOR \( i = k, \ldots, 1 \) DO

3:     \( x = d \) and \( d = x^2 \mod n \)

4:  IF \( d = 1 \) and \( x \neq 1 \) and \( x \neq n - 1 \)  RETURN TRUE

5:  IF \( b_i = 1 \)  THEN  \( d = d \cdot a \mod n \)

6:  END FOR

7:  IF \( d \neq 1 \)  RETURN TRUE

8:  RETURN FALSE
If procedure \textit{Witness}(a, n) returns TRUE then \( n \) is composite and a proof can be constructed using \( a \).
Primality testing: Miller-Rabin test.

**PROCEDURE**  MillerRabin

**INPUT:**  Odd \( n \in \mathbb{Z}^+ \), number of repetitions \( s \)

**OUTPUT:**  COMPOSITE or PROBABLY PRIME

1:  \textbf{LET} \( \{a_1, \ldots, a_s\} \) a set of randomly chosen bases

2:  \textbf{FOR} \( i = 1, \ldots, s \) \textbf{DO}

3:  \textbf{IF}  \text{Witness}(a,n)

4:  \textbf{RETURN}  COMPOSITE

5:  \textbf{ELSE}

6:  \textbf{RETURN}  PROBABLY PRIME
Primality testing: Miller-Rabin test.

- Miller-Rabin test correct when returns COMPOSITE
- When returns PROBABLY PRIME then the error is small and does not depend on $n$
Primality testing: Miller-Rabin test.

**Theorem**

If $n$ is an odd composite number, then the number of witnesses to the compositeness of $n$ is at least $(n - 1)/2$.

**NOTE:** That this includes Carmichael numbers.

**Proof.**

Show that the number of NONwitnesses is not more than $(n - 1)/2$.
Primality testing: Miller-Rabin test.

- \( \mathbb{Z}_n^\times = \{ a \in \mathbb{Z}_n \mid \gcd(a, n) = 1 \} \)
- \( \mathbb{Z}_n^\times \) is a finite abelian group.
- \( \mathbb{Z}_{15}^\times = \{1, 2, 4, 7, 8, 11, 13, 14\} \)
Show that the number of NONwitnesses is not more than \((n - 1)/2\)

- Every nonwitness \(a\): \(a^{n-1} \equiv 1 \mod n \Rightarrow \gcd(a, n) = 1 \Rightarrow a \in \mathbb{Z}_n^x\)

- For all \(b \in \mathbb{Z}_n - \mathbb{Z}_n^x\), \(b\) is a witness:
  - \(\gcd(a, n) = d > 1 \Rightarrow ax = 1 \mod n\) has no solutions
    (including \(a^{n-2}x = 1 \mod n\)) \(\Rightarrow a^{n-1} \not\equiv 1 \mod n\)
Primality testing: Miller-Rabin test.

- Let $B$ a proper subgroup of $\mathbb{Z}_n^\times$.
- $|B| \leq |\mathbb{Z}_n^\times|/2$ and since $|\mathbb{Z}_n^\times| \leq n - 1$ we have
  \[ |B| \leq \frac{n - 1}{2} \]

We show that all nonwitnesses are contained in a proper subgroup of $\mathbb{Z}_n^\times$. 
Show all nonwitnesses are in a proper subgroup of $\mathbb{Z}_n^\times$

**Case 1: There exists $x \in \mathbb{Z}_n^\times$ s.t. $x^{n-1} \not\equiv 1 \pmod{n}$**

- $B = \{ b \in \mathbb{Z}_n^\times \mid b^{n-1} = 1 \pmod{n} \}$
- $B$ is a subgroup (closed under multiplication)
- Every nonwitness $a \in B$
- But there is $x \in \mathbb{Z}_n^\times$ s.t. $x^{n-1} \not\equiv 1 \pmod{n} \Rightarrow B \neq \mathbb{Z}_n^\times$
Show all nonwitnesses are in a proper subgroup of $\mathbb{Z}_n^\times$

Case 2: For all $x \in \mathbb{Z}_n^\times$, $x^{n-1} = 1 \mod n$

- Introduction to algorithms by Cormen, Leiserson, Rivest.
Generating pseudoprimes.

**Prime number theorem**

Let \( \pi(n) = \# \{ p \in \mathbb{N} | p \leq n, p \text{ is a prime} \} \) then

\[
\lim_{n \to \infty} \frac{\pi(n)}{n / \ln n} = 1
\]

- \( \pi(n) \approx \frac{n}{\ln n} \) for large enough \( n \)

\[
\frac{x}{\ln x} \left(1 + \frac{1}{2 \ln x}\right) < \pi(x) < \frac{x}{\ln x} \left(1 + \frac{3}{2 \ln x}\right), \text{ if } x \geq 59
\]
Generating pseudoprimes.

If \( \pi(n) \approx \frac{n}{\ln n} \) then

- \( \frac{1}{\ln n} \) is an estimate of the probability that a randomly chosen integer \( n \) is prime (even less if consider odd integers)
- To obtain a prime of the same length as \( n \) we need to examine about \( \ln n \) random integers
Generating pseudoprimes.

**PROCEDURE** Pseudoprime

**INPUT:** Size of prime $B$, number of repetitions $s$

**OUTPUT:** Pseudoprime $p$, $B < p \leq 2B$

1: REPEAT

2: Generate $p$ uniform random s.t. $B < p \leq 2B$

3: IF MillerRabin($p, s$) returns PROBABLY PRIME

4: RETURN $p$
Generating pseudoprimes.

For a given $B$ and $s$ the probability of output being a prime is at least

$$1 - 2^{-s+1} \ln B$$
Generating pseudoprimes.

**Proof.**

- Let $P = \{p \mid B < p \leq 2B, p \text{ is a prime}\}$
- $|P| = \pi(2B) - \pi(B) \geq \frac{B}{2\ln B}$, where $B \geq e^6$
- Therefore,

$$\text{Prob}(p \text{ is prime}) \geq \frac{|P|}{B} \geq \frac{1}{2\ln B}$$
Generating pseudoprimes.

Proof.

- $C$ - event that random number is composite,
- $T$ - event that Miller Rabin test returned PROBABLY PRIME.
- $Pr(p \text{ is a prime}) \leq Pr(T)$
- $Pr(C|T) = Pr(C, T)/Pr(T)$
- Now we have:

\[
\frac{1}{2 \ln B} Pr(C|T) \leq Pr(p \text{ is prime})Pr(C|T) \leq Pr(T)Pr(C|T) \\
= Pr(C, T) \leq Pr(C, T)/Pr(C) \\
\leq 2^{-s}
\]

\[
Pr(C|T) \leq 2^{-s}2 \ln B
\]
Generating pseudoprimes.

\( Pr(C|T) \leq 2^{-s}2\ln B \)

- \( Pr(C|T) \) is the probability of the output being a composite number.

- Probability of the output being a prime number is

\[
1 - Pr(C|T) \geq 1 - 2^{-s}2\ln B
\]