Compositeness tests

additional material for Lecture on December 5th, 2008

Tanja Lange

Algorithm 1 (Solovay-Strassen compositeness test)
IN: Odd $n \in \mathbb{N}$, $k \in \mathbb{N}$
OUT: “$n$ is composite” or “$n$ is prime with probability at least $1 - \frac{1}{2^k}$”

1. for $i = 1$ to $k$
   (a) choose $a \in \mathbb{Z}$ randomly with $1 < a < n$
   (b) if $\gcd(a, n) \neq 1$ return “$n$ is composite”
   (c) else
      i. $c \leftarrow \left( \frac{a}{n} \right)$ (computed using Lemma 4.2 repeatedly)
      ii. $d \leftarrow a^{n-1} \bmod n$ (using a representative in $-n/2 < d < n/2$)
      iii. if $c \neq d$ return “$n$ is composite”

2. return “$n$ is prime with probability at least $1 - \frac{1}{2^k}$”

Example 2 Let $n = 711$. Like before we choose $a = 2$ and compute

\[
c = \left( \frac{2}{711} \right) = (-1)^{(711^2 - 1)/8} = 1
\]

since $711 \equiv -1 \bmod 8$ using Lemma 4.2. Next we compute $2^{710} \equiv 569 \bmod 711$ and so $d = 569$. Since $c \neq d$ we see that $n$ is composite.
As a second example we consider $n = 341$ and again choose the basis $a = 2$. We have

\[
c = \left( \frac{2}{341} \right) = (-1)^{(341^2 - 1)/8} = -1,
\]

since $341 \equiv -3 \bmod 8$. At the same time, $2^{340} \equiv 1 \bmod 341$ and so $c \neq d$ and already $a = 2$ detects $n$ as composite.
For the Carmichael number $n = 561$ we have

\[
c = \left( \frac{2}{561} \right) = (-1)^{(561^2 - 1)/8} = 1,
\]
since \(561 \equiv 1 \mod 8\). Also \(2^{280} \equiv 1 \mod 561\); so \(n\) is a pseudo-prime under the Solovay-Strassen test to the basis \(a = 2\).

For \(a = 5\) we obtain:

\[
c = \left(\frac{5}{561}\right) = \left(\frac{5}{5}\right) = \left(\frac{1}{5}\right) = 1
\]

and \(5^{280} \equiv 1 \mod 561\); and so \(n\) is detected as composite.

**Lemma 3** Let \(n\) be a composite odd integer. For at least half of all possible bases \(a\) with \(\gcd(a, n) = 1\) we have that the Solovay-Strassen test fails, i.e.

\[
\left(\frac{a}{n}\right) \neq a^{\frac{n-1}{2}} \mod n.
\]

**Proof.** Let \(A = \{a_1, \ldots, a_k\}\) be the set of \(a_i\) for which \(\left(\frac{a_i}{n}\right) \equiv a_i^{\frac{n-1}{2}} \mod n\) with \(1 \leq a_i < n\) and \(\gcd(a_i, n) = 1\).

If there exists an integer \(1 \leq b \leq n\) with \(\gcd(b, n) = 1\) and \(\left(\frac{b}{n}\right) \neq b^{\frac{n-1}{2}} \mod n\) then we have by the first property in Lemma that

\[
\left(\frac{b \cdot a_i}{n}\right) = \left(\frac{b}{n}\right) \cdot \left(\frac{a_i}{n}\right)
\]

while

\[
(b \cdot a_i)^{\frac{n-1}{2}} = b^{\frac{n-1}{2}} \cdot a_i^{\frac{n-1}{2}}
\]

and so

\[
\left(\frac{b \cdot a_i}{n}\right) \neq (b \cdot a_i)^{\frac{n-1}{2}} \mod n.
\]

Therefore, the Solovay-Strassen test detects compositeness with at least 50% of all values \(a\) if such a number \(b\) exists.

Now we show that such a number \(b\) exists. Note, that this proof uses the factorization of \(n\), so it does not help in the actual test.

Let \(n\) factor as \(n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}\), where the \(p_i\) are distinct primes and the exponents \(\alpha_i\) are positive integers. We consider two cases.

Let first one of the the exponents \(\alpha_i\) be larger than 1, e.g. \(p_1^2 \mid n\), and put \(n' = n/p_1^2\).

For \(b = 1 + \frac{n}{p_1} = 1 + p_1n'\) we have

\[
\left(\frac{b}{n}\right) = \left(\frac{1 + p_1n'}{n}\right) = \left(\frac{1 + p_1n'}{p_1^2}\right)^2 \left(\frac{1 + p_1n'}{n'}\right) = \left(\frac{1 + p_1n'}{n'}\right) = \left(\frac{1}{n'}\right) = 1.
\]

To show that \(b^{\frac{n-1}{2}} \neq 1 \mod n\) we consider powers of \(b\) using the binomial formula. Let \(j \in \mathbb{N}\). We have

\[
b^j = (1 + p_1n')^j = \sum_{i=0}^{j} \binom{j}{i} (p_1n')^i
\]

\[
\equiv 1 + j p_1 n' + \binom{2}{j} (p_1n')^2 + \ldots
\]

\[
\equiv 1 + j p_1 n' \mod n,
\]

2
because $(p_1 n')^2 = n' n \equiv 0 \mod n$ and the same holds for higher powers. This implies that $b^j \equiv 1 \mod n$ if and only if $j p_1 n' \equiv 0 \mod n$, i.e. if and only if $p_1 \mid j$. Because $p_1$ divides $n$ it does not divide $n - 1$ and therefore also not $(n - 1)/2$. Accordingly

$$\left( \frac{b}{n} \right) \neq b^{\frac{n-1}{2}} \mod n.$$ 

We now consider the case that all the exponents equal 1, i.e. $n = p_1 \cdots p_r$ is product of distinct primes. Let $1 \leq a < p_1$ be a quadratic non-residue modulo $p_1$. Put $n' = n/p_1$. By the Chinese remainder theorem there exists an integer $b$ in $1 \leq b < n$ which solves the system of equivalences

$$b \equiv a \mod p_1,$$

$$b \equiv 1 \mod n'.$$

For this $b$ we have

$$\left( \frac{b}{n} \right) = \left( \frac{b}{p_1} \right) \left( \frac{b}{n'} \right) = (-1) \left( \frac{1}{n'} \right) = -1$$

but we cannot have $b^{\frac{n-1}{2}} \equiv -1 \mod n$ since $n'$ divides $n$ by construction and

$$b^{\frac{n-1}{2}} \equiv 1 \mod n'.$$

So for both cases we have constructed a number $b$ which fails the test. □

The Fermat test and the Solovay-Strassen test both have probability $1/2$ of detecting a composite number for each iteration. The Fermat test needs one modular exponentiation per iteration while the Solovay-Strassen test needs one modular exponentiation and the computation of one Jacobi symbol per iteration. In return there are no exceptions to the Solovay-Strassen test while the Carmichael numbers are pseudo-prime for any basis in the Fermat test in spite of being composite.

The compositeness test of Miller and Rabin has probability of detecting a composite number at least $3/4$ per iteration. It uses the observation that modulo a prime $p$ there are only two solutions of $x^2 \equiv 1 \mod p$ for $-p/2 < a < p/2$. Let $p - 1 = 2^r t$, where $t$ is an odd integer and let $b \in \mathbb{Z}$ with $1 \leq b < p$. Then either $b^t \equiv 1 \mod p$ or there exists an $r' < r$ so that $b^{2^{r'} t} \equiv -1 \mod p$.

If $n$ is composite then there are more than two solutions of $x^2 \equiv 1 \mod n$. Let e.g. $n = pq$ with $p, q$ prime then the Chinese remainder theorem leads to one solution for each of the 4 choices of sign in

$$a \equiv \pm 1 \mod p,$$

$$a \equiv \pm 1 \mod q,$$

and so there are 4 solutions. If $n$ has more factors then there are more solutions.

Let $n$ split as $n - 1 = 2^r t$, where $t$ is an odd integer. Let $b \in \mathbb{Z}$ with $\gcd(b, n) = 1$. If $n$ is pseudo-prime to the basis $b$ then $b^{n-1} \equiv 1 \mod n$ but this does not imply that either $b^t \equiv 1 \mod n$ or that there exists an $r' < r$ so that $b^{2^{r'} t} \equiv -1 \mod n$ because there are more elements $a$ which are equivalent to 1 modulo $n$ when squared. So if a subsequent
squaring of \( b^t \) reaches 1 without having reached \(-1\) we know that \( n \) is composite. On top of that we detect compositeness of \( n \) if it is not pseudo-prime for a chosen basis, namely if \( b^{2^rt} \not\equiv 1 \mod n \).

This motivates the definition of strong pseudo-primes.

**Definition 4 (Strong pseudo-prime)**

Let \( n \) be an odd composite integer and let \( n - 1 = 2^rt \), with \( r \) odd.

Let \( b \in \mathbb{Z} \) with \( \gcd(b, n) \neq 1 \). If either \( b^t \equiv 1 \mod n \) or if there exists \( 0 \leq r' < r \) so that \( b^{2^rt} \equiv -1 \mod n \) then \( n \) is a strong pseudo-prime to the basis \( b \).

The above considerations have motivated the following lemma which we present without proof. The interested reader is referred to Koblitz’ book.

**Lemma 5** Let \( n \) be an odd composite integer. It is a strong pseudo-prime to at most one quarter of all possible bases \( b \).

**Algorithm 6 (Miller-Rabin compositeness test)**

**IN:** Odd \( n \in \mathbb{N} \), with \( n - 1 = 2^rt \) and \( t \) odd and \( k \in \mathbb{N} \)

**OUT:** “\( n \) is composite” or “\( n \) is prime with probability at least \( 1 - \frac{1}{4^k} \)”

1. for \( i = 1 \) to \( k \)
   
   (a) choose \( a \in \mathbb{Z} \) randomly with \( 1 < a < n \)
   
   (b) if \( \gcd(a, n) \neq 1 \) return “\( n \) is composite”
   
   (c) else if \( a^t \neq \pm 1 \mod n \)
      
      i. \( j \leftarrow 1 \)
      
      ii. while \( a^{2^jt} \neq \pm 1 \mod n \) and \( j < r \)
          
          \( j \leftarrow j + 1 \)
      
      iii. if \( a^{2^jt} \equiv 1 \mod n \) return “\( n \) is composite”
      
      iv. if \( j = r \) return “\( n \) is composite”

2. return “\( n \) is prime with probability at least \( 1 - \frac{1}{4^k} \)”

**Example 7** Let \( n = 711 \). We have \( n - 1 = 710 = 2^1 \cdot 355 \), so \( r = 1 \) and \( t = 355 \). We choose again \( a = 2 \).

We have \( a^t = 2^{355} \equiv 458 \not\equiv 1 \mod 711 \), so the iteration starts. However, \( j = 1 = r \) is reached immediately and we obtain \( n \) is composite as answer. Note that it is correct to stop the test here because either the next squaring leads to a value \( \neq 1 \) in which case the Fermat test detects \( n \) as composite or \( n \) is pseudo-prime to the basis \( a \) but reaches the value 1 without having reached \(-1\) which we identified as another criterion for compositeness.

Now consider \( n = 341 \) with \( n - 1 = 340 = 2^2 \cdot 85 \), so \( r = 2 \) and \( t = 85 \). For the basis \( a = 2 \) we have

\[
2^{85} \equiv 32 \not\equiv 1 \mod 341, \quad 2^{2 \cdot 85} \equiv 1 \mod 341,
\]

and so \( n \) is detected as composite since 1 was reached as square of 85 \( \not\equiv -1 \mod 341 \).

Finally, let \( n = 561 \) with \( n - 1 = 560 = 16 \cdot 35 \). We have

\[
2^{35} \equiv 263 \mod 561, \quad 2^{2 \cdot 35} \equiv 166 \mod 561, \quad 2^{2^2 \cdot 35} \equiv 67 \mod 561, \quad 2^{2^3 \cdot 35} \equiv 1 \mod 561,
\]

which in the last round on the first basis \( a \) detects \( n \) as composite.
Exercise 8

1. Let $n_1 = 717$. Check compositeness of $n_1$ using the Fermat test.

2. Compute $\left( \frac{7001}{14175} \right)$.

3. Prove Lemma 4.2 (the properties of the Jacobi symbol) using the properties of the Legendre symbol. Hint: study how remainders modulo 8 and 16 behave under multiplication and squaring.

4. Let $n_2 = 709$ and $n_3 = 721$. Use the Miller-Rabin test to check compositeness of $n_2$ and $n_3$ for $k = 2$. 