

Algorithmic Number Theory 3

Notes by Al Sethuraman

October 14th 2000

New and Improved Version

There could still be holes!

- Some remarks on how one might implement the Solovay-Strassen test are in order. Given an n whose primality is to be tested, one picks *at random* an integer a with $1 < a < n$. (There is much literature on random number generation—we typically generate only “pseudo” random numbers—but we will not go into this topic at this juncture.) One checks if $\gcd(a, n) = 1$, using the Euclidean Algorithm. As explained at the bottom of Page 3 of Notes **1**, this is a fast procedure, which only takes $O(k^2)$ bit operations, where $k = \log_2 n$. (Note: actually, the estimate at the bottom of Page 3 of Notes **1** namely $O(k^3)$ is too gross—it is quite easy to see that one only needs $O(k^2)$ operations for the g.c.d.) If a and n are not relatively prime, then n is clearly composite, and we are done. If not, we compute the Jacobi symbol $(\frac{a}{n})$ as explained at the end of Notes **2**, and we compute $a^{\frac{n-1}{2}} \pmod{n}$ using the repeated square method (see below). If they are not equal, we are done, else, we pick another random integer a_2 between 1 and n and repeat the test. We repeat this k times, where k is such that we are satisfied with probability $1 - (\frac{1}{2})^k$ that n is prime.

- To compute $b^r \pmod{n}$ for any r , we have the following fast algorithm called the repeated square method. Simply multiplying b by itself (and reducing modulo n) involves $O(r)$ multiplication (followed by reduction modulo n), which is exponential in the number of bits in r , and when r is large, say of the order of n , this is very expensive. Instead, one considers the binary representation of r , say $r = 2^k a_k + (2^{k-1}) a_{k-1} + \dots$, where the a_i are either 0 or 1. Then $b^r = ((b^2)^k)^{a_k} \cdot ((b^2)^{k-1})^{a_{k-1}} \dots$. For example, to compute b^7 , we first observe that $7 = 4 + 2 + 1$, so we square b and reduce mod n , multiply this result of squaring and reducing by b and set it aside, square $b^2 \pmod{n}$ from two steps ago and reduce mod n , and then multiply that with the number we set aside! Notice that there are about $\log_2 r$ squaring and reductions mod n . At each stage, one takes $b^{2^i} \pmod{n}$, which has at most k bits, and squares it further, to get an integer of about $2k$ bits, and then reduces this mod n , a process that is $O((2k)^2) + O((2k)^2) = O(k^2)$. Thus, the whole process takes $O(\log_2 r \cdot k^2)$ bit operations. When r is bounded by n (as in the Solovay-Strassen algorithm), we may view this as $O(k^3)$ —this is significantly better than brute force multiplication, which needs $O(r)$ ($= O(2^k)$ in the Solovay-Strassen algorithm) bit operations.

- We now consider a significant improvement on the Solovay-Strassen test for primality: the Miller-Rabin test. The proportion of strong liars for this test is $1/4$, which is much better than $1/2$ —since $(1/4)^k \ll (1/2)^k$ as k gets larger, one gets much higher probability of correctness of this test ($= 1 - (1/4)^k$) with k repetitions of this test than with the Solovay-Strassen test.

- So here is the Miller-Rabin test: One starts with a given n whose primality is to be tested, say of k bits, and factors $n - 1$ as $2^t s$ for suitable s odd. (As explained towards the bottom of Page 2 in Notes 1, this factorization is easy—one just reads off the number of bits on the right that are zero.) One picks an a at random with $1 < a < n$ and $(a, n) = 1$. (Checking that $(a, n) = 1$ is an $O(k^2)$ process, as explained above.) In succession, one computes $a^s, (a^s)^2, (a^s)^{2^2}, \dots, (a^s)^{2^{t-1}}, (a^s)^{2^t}$ (all mod n). We deem the test to be successful if either $a^s = 1 \pmod{n}$, or else, one of the numbers $(a^s)^2, (a^s)^{2^2}, \dots, (a^s)^{2^{t-1}}, (a^s)^{2^t}$ is $1 \pmod{n}$, and the previous number on this list is $-1 \pmod{n}$. The motivation for this test is the following:

Lemma 0.1 *When $n = p$, a prime, every a with $(a, p) = 1$ satisfies the Miller-Rabin test.*

Proof. In the group $U(\mathbf{Z}/p)$, if the order of a divides s , then $a^s = 1$, and the test will be successful. Otherwise, since $a^{p-1} = (a^s)^{2^t} = 1$, some number in the list $(a^s)^2, (a^s)^{2^2}, \dots, (a^s)^{2^{t-1}}, (a^s)^{2^t}$ will definitely be 1. Let i be minimal such that $(a^s)^{2^i} = 1$ (i is not zero by assumption). Then, $(a^s)^{2^{i-1}}$ has square equal to 1 but is not 1, and since the only square roots of 1 in $U(\mathbf{Z}/p)$ are 1 and -1 , $(a^s)^{2^{i-1}}$ must be -1 . Hence the test will be successful in this case too. ■

- When a satisfies the Miller-Rabin test, n is said to be *strong pseudoprime* to base a .
- The following theorem shows us that “ α ” for the Miller-Rabin test is $1/4$.

Theorem 0.2 *Let n be a composite number. Then, except when $n = 9$, at most a quarter of all integers a with $1 \leq a \leq n$ and $(a, n) = 1$ satisfy the Miller-Rabin test.*

Proof. We first settle a special case: when n is divisible by the square of some prime $p \geq 5$. Write $a = (a_1, \dots)$ in the decomposition $\mathbf{Z}/n \cong \mathbf{Z}/p^\alpha \times \dots$, and note that $\alpha > 1$. If a passes the Miller-Rabin test, then a^{n-1} has to be 1. In particular, in the group $U(\mathbf{Z}/p^\alpha)$, a_1^{n-1} must be 1. Thus, the order of a_1 must divide $n - 1 = p^\alpha \dots - 1$. Since the order of a_1 must also divide $\phi(p^\alpha) = p^{\alpha-1}(p - 1)$, and since p cannot divide $p^\alpha \dots - 1$, we find that the order of a_1 must divide $p - 1$. Now, if g is a generator of $U(\mathbf{Z}/p^\alpha)$, the elements in $U(\mathbf{Z}/p^\alpha)$, of order dividing $p - 1$ are precisely the powers of g^{p^α} . There are precisely $p - 1$ of these powers. Hence, at the very least, a must of the form $((g^{p^\alpha})^\lambda, \dots)$, for $\lambda = 1, \dots, p - 1$. It follows that the proportion of a 's that will satisfy the Miller-Rabin test is at most $\frac{p-1}{\phi(p)} = \frac{1}{p^{\alpha-1}}$. This is less than $1/4$ when $\alpha > 1$ and $p \geq 5$.

In fact, if $p = 3$ and $\alpha > 2$, then too, this fraction is less than $1/4$. Thus, we only have to worry about two cases: when n is square free, that is, when $n = p_1 \cdot p_2 \cdot p_3 \dots$, and when $n = 3^2 \cdot p_2 \cdot p_3 \dots$. (Actually, a computer scientist would ignore the second case, since it can be checked easily if n is divisible by 3!)

We first consider the case where $n = p_1 \cdot p_2 \cdot p_3 \dots$. Here too, we have two cases to consider: when n has at least three prime factors, and when n has exactly two prime factors. We deal with the three prime factors case first. For ease of notation, write the prime factorization of n as $n = p \cdot q \cdot r \dots$. Let $p - 1 = 2^x \alpha$, $q - 1 = 2^y \beta$, and $r - 1 = 2^z \gamma$ for odd α, β , and γ . We consider various cases below. As throughout in this section, $n - 1 = 2^t s$, with s odd.

The following is a key observation:

Lemma 0.3 *With notation as above, if $e = (a^s)^{2^u}$, for some $u \leq t$ is such that (in the decomposition of \mathbf{Z}/n into primary factors) some slot contains either 1 or some element of odd order while some other slot contains a nonidentity element, then n cannot be a strong pseudoprime to base a .*

Proof. If there is a 1 in one slot and a nonidentity element in another, then even if some further 2 power of x becomes $1 = (1, 1, \dots)$, the previous 2 power will not be $-1 = (-1, -1, \dots)$ because of the presence of a 1 in x . If there is an element of odd order (not equal to 1) in one slot and a nonidentity element in another slot, then no further 2 power of x can become $1 = (1, 1, \dots)$, since the element of odd order on raising to various powers of 2 will never yield the identity. ■

We need one more observation:

Lemma 0.4 *With the notation above, let b be any element of $U(\mathbf{Z}/p)$ that is a 2^k -th power, but not a 2^{k+1} -th power. Then $(b^s)^{2^{x-k}}$ is either 1 or an element of odd order, while $(b^s)^{2^{x-(k+1)}}$ is some nonidentity element.*

Proof. Let g be a generator of $U(\mathbf{Z}/p)$. Then $b = g^l$, where 2^k divides l , but 2^{k+1} does not divide l . Then $e = (b^s)^{2^{x-k}} = g^{sl2^{x-k}}$, and by the hypothesis on l , $sl2^{x-k}$ is divisible by 2^x , and hence, $e^\alpha = 1$, so the order of e is divisible by α . Since α is odd, we find that either e is already 1, or else, e is of odd order.

Now let $e = (b^s)^{2^{x-(k+1)}}$. Thus, $e = g^{sl2^{x-(k+1)}}$. By the hypothesis on l , we may write this as $g^{\text{odd } 2^{x-1}}$. This can never be the identity, as the order of g is *odd* 2^x , and 2^x does not divide 2^{x-1} . ■

We now proceed to the case where n is divisible by at least three primes.

Case $x = y = z$. Notice that whenever $a \in U(\mathbf{Z}/n)$ has any of the forms $(sq, sq, \text{non}sq, \dots)$, $(sq, \text{non}sq, sq, \dots)$, $(\text{non}sq, sq, sq, \dots)$, $(sq, \text{non}sq, \text{non}sq, \dots)$, $(\text{non}sq, sq, \text{non}sq, \dots)$, $(\text{non}sq, \text{non}sq, sq, \dots)$, then $(a^s)^{2^{x-1}}$ contains a 1 or an element of odd order in a suitable slot and a nonidentity element in another slot. Each of these cases hence rules out 1/8th of the elements in $U(\mathbf{Z}/n)$ (each component is a cyclic group, so exactly half the elements are squares). These cases are mutually exclusive, so a total of at least 3/4 of the elements are ruled out. So, the number of bases for which n is a strong pseudoprime is at most 1/4.

Case $x = y > z$. This time, when $a \in U(\mathbf{Z}/n)$ has any of the forms $(sq, \text{non}sq, \text{arbitrary}, \dots)$, $(\text{non}sq, sq, \text{arbitrary}, \dots)$, $(\text{non}sq, \text{non}sq, \text{arbitrary}, \dots)$ then $(a^s)^{2^{x-1}}$ contains a 1 or an element of odd order in a suitable slot and a nonidentity element in another slot. These are mutually exclusive cases, accounting for a total of 3/4 of the elements in $U(\mathbf{Z}/n)$.

Case $x > y + 1$, and $y \geq z$. Any element of the form $a = (\text{non}sq, \text{arbitrary}, \text{arbitrary}, \dots)$ is such that $(a^s)^{2^{x-1}}$ contains a 1 or an element of odd order in a suitable slot and a nonidentity element in another slot. This accounts for 1/2 of the elements in $U(\mathbf{Z}/n)$. Moreover, any element of the form $a = (sq \text{ but not a 4th power}, \text{arbitrary}, \text{arbitrary}, \dots)$ is such that

$(a^s)^{2^{x-2}}$ contains a 1 or an element of odd order in a suitable slot and a nonidentity element in another slot. There are $1/4$ of these, and these are disjoint from the previous set. Hence, there are at least $3/4$ of the elements in $U(\mathbf{Z}/n)$ for which n is not a strong pseudoprime to that base.

Case $x = y + 1$, and $y \geq z$. Any element of the form $a = (\text{nonsq}, \text{arbitrary}, \text{arbitrary}, \dots)$ is such that $(a^s)^{2^{x-1}}$ contains a 1 or an element of odd order in a suitable slot and a nonidentity element in another slot. This accounts for $1/2$ of the elements in $U(\mathbf{Z}/n)$. Moreover, any element of the form $a = (\text{sq but not 4th power}, \text{square}, \text{arbitrary}, \dots)$ is such that $(a^s)^{2^{x-2}}$ contains a 1 or an element of odd order in a suitable slot and a nonidentity element in another slot. There are $1/4 \times 1/2 = 1/8$ of these. Finally, any element of the form $(\text{sq}, \text{nonsq}, \text{arbitrary}, \dots)$ also has the same property. There are $1/4 \times 1/2 = 1/8$ of these. Together, there are $3/4$ of the elements in $U(\mathbf{Z}/n)$ for which n is not a strong pseudoprime to that base.

Now we deal with the case when $n = pq$ for distinct primes p and q . As before, $p = 2^x \alpha$ and $q = 2^y \beta$ for α and β odd. The proofs for the cases $x > y + 1$ and $x = y + 1$ are identical with the ones given above for the $n = pqr$ case: notice that those proofs above really did not depend on the third prime q . Thus, we only need to deal with the case where $x = y$ (and here, note that the proof above, in the sub-case where $x = y = z$ depended crucially on the existence of the third prime).

First, we need the following:

Lemma 0.5 *With notation as above, assume that $\alpha > \beta$. Then α does not divide s .*

Proof. We have $n - 1 = (2^x \alpha + 1)(2^x \beta + 1) - 1$, and this works out to $2^x(2^x \alpha \beta + \alpha + \beta)$. Of course, $2^x \alpha \beta + \alpha + \beta$ will have further powers of 2 that divide it, but in any case, s will divide $2^x \alpha \beta + \alpha + \beta$. Hence, if α divides s , then α will divide $2^x \alpha \beta + \alpha + \beta$, which means that $\alpha | \beta$, a contradiction, as $\alpha > \beta$. ■

As before, anything of the form $((\text{sq}, \text{nonsq})^s)^{2^{x-1}}$ and $((\text{nonsq}, \text{sq})^s)^{2^{x-1}}$ will contain a nonidentity element in one slot, and either a 1 or an element of odd order in the other slot. Hence, such an element will fail the Miller-Rabin test. This accounts for $1/4 + 1/4 = 1/2$ the elements.

Now consider the combination $(\text{nonsq}, \text{nonsq})$. We claim that any such combination such that $((\text{nonsq}, \text{nonsq})^s)^{2^{x-1}} \neq (-1, -1)$ will fail the Miller-Rabin test. For, suppose that g generates $U(\mathbf{Z}/p)$ and h generates $U(\mathbf{Z}/q)$. Then our element looks like (g^λ, h^μ) for some odd integers $\lambda \leq p - 1$ and $\mu \leq q - 1$. Now suppose that $((g^\lambda, h^\mu)^s)^{2^{x-1}} \neq (-1, -1)$. Notice that $(g^{s\lambda})^{2^{x-1}}$ cannot be the identity, as $g^{2^{x-1}}$ has order 2α , and 2α cannot divide $s\lambda$ as both s and λ are odd. Thus, $((g^\lambda, h^\mu)^s)^{2^{x-1}}$ equals (a, b) , where neither slot is 1, and both are not -1 . It follows that (a^2, b^2) is not $(1, 1)$, and further, since a^2 is just $(g^{2x})^{s\lambda}$ and (g^{2x}) has order α , a^2 has order dividing α . Similarly, b^2 has order dividing β . Thus, (a^2, b^2) is of odd order (and not equal to the identity), and repeated squaring will never produce $(1, 1)$.

Thus, we need to count the λ and μ such that $((g^\lambda, h^\mu)^s)^{2^{x-1}} = (-1, -1)$ and rule these out.

The various 2^{x-1} -th roots of -1 are of the form $(g^\alpha)^{\alpha'}$ and $(h^\beta)^{\beta'}$ for odd α' and odd β' . (This follows from the fact the group of elements of order 2^x are generated by g^α and h^β .) Hence, we must have $g^{\lambda s} = g^{\alpha\alpha'}$ and $h^{\mu s} = h^{\beta\beta'}$. Thus, $2^x\alpha$ must divide the difference $\lambda s - \alpha\alpha'$ and $2^x\beta$ must divide $\mu s - \beta\beta'$. In particular, $\alpha|\lambda s$ and $\beta|\mu s$. Thus, we must pick λ and μ such that this does not happen.

Let $r' = \gcd(\alpha, s)$, and let $r = \alpha/r'$. By the lemma, α does not divide s , so $r > 1$. In particular, $r \geq 3$ (as the relevant integers are all odd). But it is clear that at least half the odd integers in the list $1, 3, 5, \dots, 2^x\alpha - 1$ cannot be multiples of r (as $r \geq 3$), so (*half the nonsq, nonsq*) will fail the test. This accounts for another $1/8$ the elements, making $5/8$ failures so far.

Now say $x \geq 2$. Then among the elements of the form (sq, sq) , another $5/8$ will fail the test, using exactly the same arguments as above. Thus, there will be $1/4 \times 5/8 = 5/32$ additional failures. All told, we have $5/8 + 5/32 = 25/32 > 3/4$ failures.

Now assume that $x = 1$. We consider the subgroup of elements of the form (sq, sq) . Every element in the first slot has order dividing α , and every element in the second has order dividing β , so this group has odd order (which divides $\alpha\beta$). Let (a, b) be any element of this subgroup such that $(a, b)^s \neq (1, 1)$. Then you will never get $(1, 1)$ on repeated squaring, since a^s and b^s are of odd order, and at least one is not the identity. Let $a = g^{2\lambda}$ and $b = h^{2\mu}$. We need to rule out those λ and μ such that $(g^{2\lambda})^s = 1$ and $(h^{2\mu})^s = 1$. Now $(g^{2\lambda})^s = 1$ means that 2α divides $2\lambda s$, i.e., that α divides λs . As before, let $r' = \gcd(\alpha, s)$, and let $r = \alpha/r'$. Then, by the lemma, $r \geq 3$. We choose λ from the set $1, 2, 3, \dots, \alpha$ so that r does not divide λ . Since $r \geq 3$, at most $\{\alpha/3\}$ of the elements ($\{\}$ stands for the greatest integer) in this set will be multiples of r , so the non-multiples of r will at least $2\alpha/3$. Hence, at least two-thirds of the combinations (sq, sq) will fail the Miller-Rabin test. This accounts for another $1/6$ failures, making at least $5/8 + 1/6 = 19/24$ failures.

Finally, we deal with the case where $n = 9 \cdot p_1 \cdot p_2 \cdots$ (which most computer scientists wouldn't really care about!). If n were divisible by three distinct primes, then the arguments just given for when n is squarefree apply here too. (For that argument to work, all we needed is that $U(\mathbf{Z}/n)$ is the direct product of at least three cyclic groups; note that $U(\mathbf{Z}/9)$ is also cyclic.) So we only have to worry about when $n = 9$ and $n = 9p$ for some prime p . The case $n = 9$ is easy to dispose of: $U(\mathbf{Z}/9)$ is cyclic of order 6, so if $a^8 = 1$ for some element $a \in U(\mathbf{Z}/9)$, then a must have order 1 or 2, so it must be the identity, or -1 , where g is some generator of $U(\mathbf{Z}/9)$. Both these elements satisfy the Miller-Rabin test, so $1/3$ of the elements of $U(\mathbf{Z}/9)$ satisfy the test. (This provides the exception in the statement of the theorem.)

For $n = 9p$, suppose n is a pseudoprime to base $a = (u, v)$, with $u \in U(\mathbf{Z}/9)$ and $v \in U(\mathbf{Z}/p)$. We should have $u^{n-1} = 1$ so $o(a)|n - 1$. Of course, $o(a)|6$ as well. But $n - 1 = 9p - 1$, so 3 does not divide $n - 1$. It follows that $o(a) = \pm 1$. This rules out already $2/3$ of the elements. By our lemma, any a of the form $(1, \text{nonsq})$ will not pass this test, which rules out a further $1/12$. Together, at least $3/4$ of the elements will fail the test.

This proves the theorem. ■