THE SOLOVAY–STRASSEN TEST

KEITH CONRAD

1. Introduction

The Jacobi symbol satisfies many formulas that the Legendre symbol does, such as these: for $a, b \in \mathbf{Z}$ and odd $m, n \in \mathbf{Z}^+$,

(1) $a \equiv b \bmod n \Rightarrow (\frac{a}{n}) = (\frac{b}{n})$,
(2) $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$,
(3) $(\frac{-1}{n}) = (-1)^{(n-1)/2}$ and $(\frac{2}{n}) = (-1)^{(n^2-1)/8}$,
(4) $(\frac{n}{m}) = (-1)^{(m-1)/2\cdot(n-1)/2}(\frac{m}{n})$.

But there is one basic rule about Legendre symbols that is not listed above for the Jacobi symbol: an analogue of Euler's congruence $a^{(p-1)/2} \equiv (\frac{a}{p}) \bmod p$ if $1 \leq a \leq p-1$. The natural analogue of this for an odd composite modulus n would be

$$1 \leq a \leq n-1 \Longrightarrow a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n. \tag{1.1}$$

It turns out that this congruence has *lots* of counterexamples for a whenever n is odd and composite (Corollary 3.2 below), and this will lead to a probabilistic primality test.

2. Euler witnesses

Definition 2.1. If n is an odd positive integer then any integer $a \in \{1, \ldots, n-1\}$ such that either (i) $(a, n) > 1$ or (ii) $(a, n) = 1$ and $a^{(n-1)/2} \not\equiv (\frac{a}{n}) \bmod n$ is called an *Euler witness* for n.

If n is an odd prime then neither (i) nor (ii) holds for any a from 1 to $n-1$, so n has no Euler witnesses. Therefore the existence of a single Euler witness for n proves n is composite, but does not tell us how to factor n.

The condition $(a, n) > 1$ is equivalent to $(\frac{a}{n}) = 0$, so we don't need to test if $(a, n) > 1$ or $(a, n) = 1$ separately when checking if a is an Euler witness: the process of testing whether or not $a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n$ will reveal if $(a, n) > 1$ when the right side is 0.

It's a little easier to say when a is *not* an Euler witness for n than when it is an Euler witness: not being an Euler witness means

$$(a, n) = 1 \text{ and } a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n, \tag{2.1}$$

and the condition that $(a, n) = 1$ is equivalent to $(\frac{a}{n}) = \pm 1$.

Euler witnesses are a more general concept than Fermat witnesses: every Fermat witness is an Euler witness The proof is left to the reader. (Hint: prove the contrapositive, that a number that is not an Euler witness is not a Fermat witness.)

Example 2.2. Let $n = 1387$. Since

$$2^{(n-1)/2} = 2^{693} \equiv 512 \not\equiv \pm 1 \bmod 1387,$$

2 is an Euler witness for n. It is not a Fermat witness since $2^{n-1} \equiv 1 \bmod n$. The number of Euler witnesses for n is 1224, which is about 88.2% of the nonzero numbers mod n.

Example 2.3. Let $n = 49141$. From the table below 5 is an Euler witness.

a	$a^{(n-1)/2} \bmod n$	$(\frac{a}{n})$
2	-1	-1
3	1	1
4	1	1
5	8163	1

The number of Euler witnesses for n is 36972, which is about 75.2% of the nonzero numbers mod n.

Example 2.4. Let $n = 75361$. From the table below 7 is an Euler witness.

a	$a^{(n-1)/2} \bmod n$	$(\frac{a}{n})$
2	1	1
3	1	1
4	1	1
5	1	1
6	1	1
7	1	-1

Unlike the previous two examples, the first Euler witness $a = 7$ has $a^{(n-1)/2} \equiv \pm 1 \bmod n$, but the sign is not $(\frac{a}{n})$. The congruence in (1.1) is *more precise* than $a^{(n-1)/2} \equiv \pm 1 \bmod n$.

The number of Euler witnesses for n is 46560, which is about 61.7% of the nonzero numbers mod n.

3. The theorems of Solovay and Strassen

If we to try to determine if n is prime with the Fermat test by seeking a counterexample to $a^{n-1} \equiv 1 \bmod n$ among the numbers from 1 to $n-1$, we know the proportion of counterexamples (the Fermat witnesses for n) is greater than 50% if n is composite and not a Carmichael number (that is, if n is composite and $a^{n-1} \not\equiv 1 \bmod n$ for some a relatively prime to n). But if n is a Carmichael number, the only counterexamples to $a^{n-1} \equiv 1 \bmod n$ are the a for which $(a, n) > 1$, and the proportion of such a could be very small. The following theorem and corollary, due to Solovay and Strassen, say this problem never occurs for Euler's congruence: there is nothing like Carmichael numbers for (1.1).

Theorem 3.1 (Solovay–Strassen)**.** *Let n be an odd composite positive integer. There is an integer a such that $(a, n) = 1$ and $a^{(n-1)/2} \not\equiv (\frac{a}{n}) \bmod n$.*

The key point is that $a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n$ fails for some a that is *relatively prime* to n.

Proof. We take two cases: n is squarefree and n has a repeated prime factor.

Suppose n is composite and squarefree, so $n = p_1 p_2 \cdots p_r$ with $r \geq 2$ (n is not prime!) and the p_i's are distinct odd primes. Half the nonzero numbers mod p_1 are not squares, so there is $b \in \mathbf{Z}$ such that $(\frac{b}{p_1}) = -1$. By the Chinese remainder theorem some $a \in \mathbf{Z}$ satisfies

$$a \equiv b \bmod p_1, \quad a \equiv 1 \bmod p_2 \cdots p_r.$$

Then a is relatively prime to p_1 and to $p_2 \cdots p_r$, so $(a, n) = 1$. Also $(\frac{a}{p_1}) = (\frac{b}{p_1}) = -1$ and $(\frac{a}{p_i}) = (\frac{1}{p_i}) = 1$ for $i > 1$, so

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right) = \left(\frac{a}{p_1}\right) = -1.$$

Assume $a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n$, so $a^{(n-1)/2} \equiv -1 \bmod n$. Since p_2 divides n, we can reduce the congruence $a^{(n-1)/2} \equiv -1 \bmod n$ to modulus p_2, getting

$$1 \equiv -1 \bmod p_2$$

since $a \equiv 1 \bmod p_2$. This is a contradiction since the modulus p_2 is greater than 2.

Now suppose n has a repeated prime factor,[1] say p. Then $n = p^k m$ where $k \geq 2$ and $(p, m) = 1$. By the Chinese remainder theorem, there is an $a \in \mathbf{Z}$ satisfying

$$a \equiv 1 + p \bmod p^2, \quad a \equiv 1 \bmod m.$$

Therefore a is not divisible by p and $(a, m) = 1$, so $(a, n) = 1$. If $a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n$ then squaring gives us $a^{n-1} \equiv 1 \bmod n$, and we're going to show that is impossible. Reduce the congruence to modulus p^2 (a factor of n) to obtain $a^{n-1} \equiv 1 \bmod p^2$. Since $a \equiv 1+p \bmod p^2$ we get $(1+p)^{n-1} \equiv 1 \bmod p^2$. Using the binomial theorem, $(1+p)^{n-1} \equiv 1+(n-1)p \bmod p^2$, so $1 + (n-1)p \equiv 1 \bmod p^2$. Subtracting 1 from both sides, $(n-1)p \equiv 0 \bmod p^2$, so $n - 1 \equiv 0 \bmod p$. But n is a multiple of p, so we have a contradiction. □

Corollary 3.2. *Let $n > 1$ be an odd integer.*

(1) *For prime n, $|\{1 \leq a \leq n-1 : a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n\}| = n - 1$.*

(2) *For composite n, $|\{1 \leq a \leq n-1 : (a, n) = 1$ and $a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n\}| < \dfrac{n-1}{2}$.*

Proof. Part (1) is true by Euler's congruence for the Legendre symbol. To prove (2), first recall that $(\frac{a}{n}) = \pm 1$ if $(a, n) = 1$ and $(\frac{a}{n}) = 0$ if $(a, n) > 1$. Set

$$\begin{aligned} A &= \left\{1 \leq a \leq n-1 : (a,n) = 1 \text{ and } a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n\right\}, \\ B &= \left\{1 \leq a \leq n-1 : (a,n) = 1 \text{ and } a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \bmod n\right\}, \\ C &= \{1 \leq a \leq n-1 : (a,n) > 1\}. \end{aligned}$$

The sets A, B, and C are disjoint and fill up all the integers from 1 to $n-1$. The set A is not empty since $1 \in A$. The set C is not empty since n is composite. By Theorem 3.1, B is provably not empty too. We want to show $|A| < (n-1)/2$.

Pick a number in B, say b_0. We will show the set $Ab_0 = \{ab_0 \bmod n : a \in A\}$ is inside B, where "$ab_0 \bmod n$" means the remainder when we divide ab_0 by n. Indeed, for any $a \in A$, the product ab_0 is relatively prime to n and

$$(ab_0)^{(n-1)/2} \equiv a^{(n-1)/2} b_0^{(n-1)/2} \equiv \left(\frac{a}{n}\right) b_0^{(n-1)/2} \bmod n.$$

Either $ab_0 \bmod n$ is in A or B. If $ab_0 \bmod n \in A$ then $(ab_0)^{(n-1)/2} \equiv (\frac{ab_0}{n}) = (\frac{a}{n})(\frac{b_0}{n}) \bmod n$, so $(\frac{a}{n})(\frac{b_0}{n}) \equiv (\frac{a}{n}) b_0^{(n-1)/2} \bmod n$. Since $(a, n) = 1$ we have $(\frac{a}{n}) = \pm 1$, so we can cancel $(\frac{a}{n})$ on both sides of the congruence to get $(\frac{b_0}{n}) \equiv b_0^{(n-1)/2} \bmod n$, which contradicts b_0 being in B. Thus $ab_0 \bmod n \in B$ for all $a \in A$, so $Ab_0 \subset B$.

[1]The proof of Theorem 3.1 in the original paper of Solovay and Strassen [9] did not cover a special case of this, when n is a perfect square. They filled in that gap later [10].

For a and a' in A, if $ab_0 \equiv a'b_0 \bmod n$ then cancel b_0 to get $a \equiv a' \bmod n$, so $a = a'$ because numbers in A lie strictly between 0 and n. Thus the number of elements in Ab_0 is $|A|$, so from $Ab_0 \subset B$ we have $|A| = |Ab_0| \leq |B|$. Therefore

$$n - 1 = |A| + |B| + |C| \geq |A| + |A| + 1 > 2|A|,$$

so $n - 1 > 2|A|$. Thus $|A| < (n-1)/2$. □

Theorem 3.3. *Let $n > 1$ be an odd integer. The proportion of integers from 1 to $n-1$ that are Euler witnesses for n is 0% if n is prime and over 50% if n is composite.*

Proof. An odd prime number has no Euler witnesses by Euler's congruence. The second part of Corollary 3.2(2) tells us that if n is composite then the proportion of integers from 1 to $n-1$ that are not Euler witnesses for n is less than 50%, so the proportion of Euler witnesses for n in this range is greater than 50%. □

The dichotomy between the proportion of Euler witnesses when n is prime or composite is very impressive. It leads to the **Solovay–Strassen test** for checking if an odd integer $n > 1$ is prime, based on the high chances of finding an Euler witness for n when n is composite compared to the nonexistence of Euler witnesses when n is prime.

(1) Pick an integer $t \geq 1$ to be the number of trials for the test.
(2) Randomly pick an integer a from 1 to $n-1$.
(3) If (2.1) is not true for a then stop the test and declare (correctly) "n is composite."
(4) If (2.1) is true for a then go back to step 2.
(5) If the test runs for t trials without terminating then say "n is prime with probability at least $1 - 1/2^t$."

The value $1 - 1/2^t$ in the last step of the test comes from the fact that over half the numbers from 1 to $n-1$ are Euler witnesses for n if n is composite. Not finding an Euler witness after t trials, if n were composite, is as likely as flipping a fair coin t times and having the same side come up each time, which has probability $1/2^t$. In fact it is *less likely* than that since the proportion of Euler witnesses is over 50%. Therefore the "probability" that n is prime if no Euler witness for n is found after t trials is *greater than* $1 - 1/2^t$. This heuristic reasoning about probability is not quite correct; we made an error related to conditional probability (there is no error in the Solovay–Strassen test, but only in the probabilistic heuristic for it). In practice the error is not that important so we won't emphasize it, but see Appendix A for the details if you are interested.

In the Solovay–Strassen test $a \in \{1, \ldots, n-1\}$ is picked randomly, not consecutively. In part this is to avoid redundant information. For instance, in Example 2.4 the entries for $a = 4$ and $a = 6$ are completely determined by those for $a = 2$ and $a = 3$ because if the congruence $a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n$ and condition $(a, n) = 1$ hold for two values of a then they hold for their product.

Example 3.4. Let $n = 56052361$. In the table below we list randomly chosen a from 1 to $n-1$ (chosen by a computer) and find a mismatch in (1.1) after 3 trials, which proves n is composite. However, we do not get a factorization of n from this: knowing a number is composite is not the same as knowing how it factors.

a	$a^{(n-1)/2} \bmod n$	$(\frac{a}{n})$
40715161	1	1
18267097	1	1
55146139	1	-1

By a brute force computation, the number of Euler witnesses for n is 27783000, which is just over half the numbers from 1 to $n-1$: $\frac{27783000}{56052360} \approx .5043$. So the lower bound of at least half the numbers being Euler witnesses for an odd composite number seems like a pretty sharp bound.

The 50% lower bound for the proportion of Euler witnesses for odd composites is probably sharp: if $6k+1$, $12k+1$, and $18k+1$ are all prime then the proportion of Euler witnesses for $(6k+1)(12k+1)(18k+1)$ tends to 50% if we can let $k \to \infty$. (It is believed that $6k+1$, $12k+1$, and $18k+1$ are all prime infinitely often.)

Example 3.5. Let $n = 2301745249$. When I used a computer to pick random numbers from 1 to $n-1$ I got $a = 325244385$ as the first choice, and $a^{(n-1)/2} \equiv 1 \bmod n$ while $(\frac{a}{n}) = -1$, so n is provably composite.

Example 3.6. Let $n = 7427466391$. In the table below we find after trying 10 *random* values of a from 1 to $n-1$ that the Solovay–Strassen test reveals no Euler witnesses.

a	$a^{(n-1)/2} \bmod n$	$(\frac{a}{n})$
3402235571	1	1
2277339183	1	1
3511612661	1	1
1892495979	-1	-1
735536755	1	1
966099371	-1	-1
3288169902	1	1
3037671250	-1	-1
270193898	1	1
7427466390	-1	-1

If n were composite then the chance of this happening is comparable to flipping a coin 10 times and getting only heads, which has probability $1/2^{10} \approx .00097$, so it is natural to believe n is prime, but the table of data is not a proof of that. (The number n really is prime, which a computer can check quickly for a 10-digit number like n.)

Example 3.7. The 14th Fermat number $2^{2^{14}}+1$ is the product of the 54-digit number

$$116928085873074369829035993834596371340386703423373313 \tag{3.1}$$

and a second number with 4880 digits. The second number is composite by the Fermat test, since a computer can show 3 is a Fermat witness for it. (No nontrivial factor of the second number is known.) Is the factor in (3.1) prime or is it composite?

Running the Fermat test on the number in (3.1) with the help of a random number generator to select a in the Fermat test, I found no Fermat witnesses for (3.1) after 100 trials. This makes a very compelling probabilistic argument that the number in (3.1) is prime or a Carmichael number. To convince ourselves that this number is prime, we use the Solovay–Strassen test. Running the Solovay–Strassen test 100 times with a random number generator to select a, I found no Euler witnesses. The probability that would happen if the number were composite is heuristically less than $1/2^{100}$. We should be morally convinced that the number in (3.1) is prime by these results, and in fact we should already be convinced after 20 trials of the Solovay–Strassen test without finding an Euler witness. Since (3.1) has less than 100 digits, it can be proved to be prime on a computer with primality proving algorithms that we do not discuss here.

Historically, the Solovay–Strassen test was the first probabilistic primality test. The Fermat test is not a probabilistic primality test because Carmichael numbers can look like primes when running the Fermat test even though they are not prime. Shortly after the Solovay–Strassen test appeared it was eclipsed by the Miller–Rabin test [6], [7], which is easier to implement (no Jacobi symbols are needed) and is more effective: every Euler witness is a "Miller–Rabin witness" and the proportion of Miller–Rabin witnesses for an odd composite number turns out to be at least 75%, not just at least 50%.

Theorem 3.1, which says there is no analogue of Carmichael numbers for the Solovay–Strassen test, was known before the work of Solovay and Strassen. It had been proved a few years earlier by Lehmer [5] and Selfridge (unpublished, see [4, p. 269]), and ten years earlier for the case of nonsquare n by Artjuhov [2, Theorem E, p. 362]. Artjuhov and Lehmer both observed that in practice an Euler witness for an odd composite number can be found quickly, but the idea of Corollary 3.2 and using it to make Theorem 3.1 into a probabilistic algorithm for primality was original to Solovay and Strassen.

4. Making Solovay–Strassen into a deterministic primality test

The Solovay–Strassen test in the form we have presented it is a probabilistic primality test: it produces an Euler witness for an odd composite number with very high probability if we run the test even for 10 trials, but if we don't find an Euler witness after 10 trials we are not assured that the number is prime. It turns out that the Solovay–Strassen test can be made into a deterministic primality test if we assume the truth of one of the most difficult unsolved problems in mathematics, called the Generalized Riemann Hypothesis (for Dirichlet L-functions). We will not explain here the Generalized Riemann Hypothesis, often abbreviated to GRH, but here is its connection to the Solovay–Strassen test.

Theorem 4.1. *If the Generalized Riemann Hypothesis is true then any odd composite positive integer n has an Euler witness that is at most $2(\log n)^2$.*

Proof. See [3]. □

This theorem, in the form above with coefficient 2 on $(\log n)^2$, is due to Eric Bach in his 1985 Ph.D. thesis. It had been proved a few years earlier by Oesterlé [8] with coefficient 70 instead of 2. Theorem 4.1 implies that if $n > 1$ is odd and we don't find an Euler witness for n among the integers up to $2(\log n)^2$ then n must be prime *if* GRH is true.

Example 4.2. For the number n in (3.1) we have $2(\log n)^2 \approx 29862.4$. A computer can check in a few seconds that there are no Euler witnesses for n among the positive integers up to 29862, which would prove n is prime if we accept GRH.

Assuming GRH holds, the Solovay–Strassen test on an odd number $n > 1$ becomes a deterministic test where the number of trials required is at most a power of $\log n$, there is no need for random inputs (test all a up to $2(\log n)^2$), and the number of steps needed in each trial (that is, to compute $a^{n-1} \bmod n$ by repeated squaring and to compute $(\frac{a}{n})$ by Jacobi reciprocity in order to verify or refute (2.1)) is also bounded by a power of $\log n$. This means the deterministic Solovay–Strassen test runs in polynomial time, which would make it a good algorithm in theory, and it would also be good in practice. Unfortunately this good situation requires assuming GRH, which remains unproved. About 20 years after Bach's theorem, a polynomial time primality test not depending on any unproved conjectures was established by Agrawal, Kayal, and Saxena [1]. It is called the AKS primality test, after its authors. While of theoretical importance, the AKS test is not used. Other deterministic

primality tests that are believed to run in polynomial time but are not yet proved to do so run much faster in practice than AKS.

5. A weaker form of the Solovay–Strassen test

The Solovay–Strassen test is a powerful improvement on the Fermat test partly because it has no analogue of Carmichael numbers. That is, while there are infinitely many composite $n > 1$ such that $(a, n) = 1 \Longrightarrow a^{n-1} \equiv 1 \bmod n$ for all a, there are no odd composite n such that $(a, n) = 1 \Longrightarrow a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n$ for all a. When $(a, n) = 1$ the Jacobi symbol $(\frac{a}{n})$ has values ± 1, so consider the following weaker form of (2.1): check for $1 \leq a \leq n-1$ if

$$a^{(n-1)/2} \equiv \pm 1 \bmod n. \tag{5.1}$$

That is, we don't bother checking if the right side is a sign in a systematic way, but just check if it is a sign or not a sign.

For odd prime n, (5.1) is true for all a from 1 to $n-1$, so if for odd $n > 1$ we find an $a \in \{1, \ldots, n-1\}$ such that $a^{(n-1)/2} \not\equiv \pm 1 \bmod n$ then n must be composite. It is left to the reader to check that if $n > 1$ is odd and there is some $a \in \{1, \ldots, n-1\}$ such that $(a, n) = 1$ and $a^{(n-1)/2} \not\equiv \pm 1 \bmod n$, then for over 50% of $a \in \{1, \ldots, n-1\}$, (5.1) is not true. This suggests the following primality test on odd $n > 1$.

(1) Randomly pick an integer a from 1 to $n-1$.
(2) If (5.1) is not true for a then stop the test and declare (correctly) "n is composite."
(3) If (5.1) is true for a then go back to step 1.
(4) If the test runs many times without terminating then say "n is probably prime."

Unfortunately, this test has an analogue of Carmichael numbers: there are odd composite $n > 1$ such that $(a, n) = 1 \Longrightarrow a^{(n-1)/2} \equiv \pm 1 \bmod n$, the first such n being 1729. This makes a primality test based on contradicting (5.1) subject to a similar defect as in the Fermat test, which is based on contradicting $a^{n-1} \equiv 1 \bmod n$. However, there is an unexpected twist when (5.1) holds for all a relatively prime to n and n is composite.

Theorem 5.1. *For odd composite $n > 1$ the following conditions are equivalent.*
1) *For all $a \in \mathbf{Z}$, if $(a, n) = 1$ then $a^{(n-1)/2} \equiv \pm 1 \bmod n$.*
2) *The number n is squarefree and for primes p, $p \mid n \Longrightarrow (p-1) \mid (n-1)/2$.*
3) *For all $a \in \mathbf{Z}$, if $(a, n) = 1$ then $a^{(n-1)/2} \equiv 1 \bmod n$.*

That the first and third conditions are equivalent is a surprise!

Proof. (1) $\Longrightarrow$ (2): From (1), if $(a, n) = 1$ then $a^{n-1} \equiv 1 \bmod n$, so n is a Carmichael number. In particular, n is squarefree and for all primes p, if $p \mid n$ then $(p-1) \mid (n-1)$. We want to show $(p-1) \mid (n-1)/2$. Write $n-1 = (p-1)m_p$. If m_p is even then $p-1$ is a factor of $(n-1)/2$. Suppose m_p were odd. Then if $(a, n) = 1$ we have $a^{(n-1)/2} = a^{(p-1)m_p/2} \equiv (\frac{a}{p})^{m_p} \bmod p$ ($p \neq 2$ since n is odd), and $(\frac{a}{p})^{m_p} = (\frac{a}{p})$ since m_p is odd. There is an integer b such that $(\frac{b}{p}) = -1$, so we can choose a by the Chinese remainder theorem to satisfy

$$a \equiv b \bmod p, \quad a \equiv 1 \bmod n/p$$

since p and n/p are relatively prime (n is squarefree). From the congruences we have $(a, n) = 1$, so by our previous calculations $a^{(n-1)/2} \equiv (\frac{a}{p}) \bmod p$, and $(\frac{a}{p}) = (\frac{b}{p}) = -1$. Thus

$a^{(n-1)/2} \equiv -1 \bmod p$. At the same time from $a \equiv 1 \bmod n/p$ we have $a^{(n-1)/2} \equiv 1 \bmod n/p$. The two congruence conditions

$$a^{(n-1)/2} \equiv -1 \bmod p, \quad a^{(n-1)/2} \equiv 1 \bmod n/p$$

together are inconsistent with having $a^{(n-1)/2} \equiv \pm 1 \bmod n$: if the right side were 1 then reducing it mod p makes $-1 \equiv 1 \bmod p$, and if the right side were -1 then reducing it mod n/p makes $1 \equiv -1 \bmod n/p$. This is a contradiction since $p > 2$ and $n/p > 2$ (here we use that n is odd and not prime).

(2) $\Longrightarrow$ (3): Since n is squarefree it suffices to show $a^{(n-1)/2} \equiv 1 \bmod p$ for all primes $p \mid n$. If $(a, n) = 1$ then $(a, p) = 1$, so $a^{(n-1)/2} \equiv 1 \bmod p$ by Fermat's little theorem, as $(n-1)/2$ is a multiple of $p - 1$.

(3) $\Longrightarrow$ (1): Trivial. □

Numbers n fitting the conditions of Theorem 5.1 must be Carmichael numbers, but of a very special type. The first three such numbers are 1729, 2465, and 15841, which are the third, fourth, and ninth Carmichael numbers. The proof that there are infinitely many Carmichael numbers also shows there are infinitely many numbers n as in Theorem 5.1.

Theorem 5.1 shows odd composite n such that $a^{(n-1)/2} \equiv \pm 1 \bmod n$ whenever $(a, n) = 1$ behave differently from odd prime n: for prime n we have $a^{(n-1)/2} \equiv -1 \bmod n$ with 50% probability each time we randomly pick a, while for such composite n we will never see $a^{(n-1)/2} \equiv -1 \bmod n$. This suggests a modification to the test above.

(1) Randomly pick an integer a from 1 to $n - 1$.
(2) If (5.1) is not true for a then stop the test and declare (correctly) "n is composite."
(3) If (5.1) is true for a then go back to step 1.
(4) If the test runs many times without terminating and we find $a^{(n-1)/2} \equiv -1 \bmod n$ at least once then say "n is probably prime."
(5) If the test runs many times without terminating and we find $a^{(n-1)/2} \equiv 1 \bmod n$ each time then say "n is probably composite."

Appendix A. Probabilistic Tests and Bayes' Rule

After we introduced the Solovay–Strassen test we said that if the test for n runs t times without finding an Euler witness then we should consider n to be prime with "probability" greater than $1 - 1/2^t$. However, there is a mistake in that. It uses Corollary 3.2(2) to estimate the probability of t runs of the Solovay–Strassen test not producing an Euler witness for n *given* that n is composite, rather than the probability of n being composite *given* that t runs of the Solovay–Strassen test don't produce an Euler witness for n. Mixing up the two types of probabilities – "Event 1 given Event 2" and "Event 2 given Event 1" – is an error about conditional probability and it can be fixed using Bayes' rule.

For two outcomes A and B from experiments (not necessarily the same experiment), we write $\Pr(A)$ for the probability that A occurs and $\Pr(A|B)$ for the probability that A occurs *given* that B occurs. For example, if we roll dice and let A be the outcome "1" and B be the outcome "odd", then $\Pr(A) = 1/6$ but $\Pr(A|B) = 1/3$ since when the outcome is odd the only outcomes are 1, 3, or 5. We call $\Pr(A|B)$ a conditional probability, since it tells us the probability of A conditioned on B happening. Its formula (or definition, really) is

$$\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)}.$$

In the example of dice, for instance, $\Pr(B) = 1/2$ and $\Pr(A \cap B) = 1/6$ (because $A \subset B$), so $\Pr(A \cap B)/\Pr(B) = (1/6)/(1/2) = 2/6 = 1/3$. If A' is the outcome complementary to A, so $\Pr(A') = 1 - \Pr(A)$, then also $\Pr(A'|B) = 1 - \Pr(A|B)$: $A \cap B$ and $A' \cap B$ are complementary in B, so $\Pr(B) = \Pr(A \cap B) + \Pr(A' \cap B)$; now just divide by $\Pr(B)$ to get $1 = \Pr(A|B) + \Pr(A'|B)$. (Warning: It is false in general that $\Pr(A|B') = 1 - \Pr(A|B)$, where B' is the event complementary to B.)

Let's return now to the Solovay–Strassen test. For an integer $n \geq 2$, we are interested in the following possible events:

- X: n is prime,
- X': n is composite,
- Y_t: the Solovay-Strassen test is run t times without finding an Euler witness for n.

(We could write X_n, X'_n, and $Y_{n,t}$ to indicate the dependence on n, but leave it out to avoid cluttering the notation.) Note X and X' are complementary. What we want to know is the "probability" that n is prime if no Euler witness is found after t tests, and that is $\Pr(X|Y_t)$. The "probability" that n is composite if no Euler witness is found after t tests is $\Pr(X'|Y_t) = 1 - \Pr(X|Y_t)$. Corollary 3.2(2) does not tell us *either* of these probabilities: rather, it tells us that *if* n is composite then the "probability" of not finding an Euler witness for n after t trials is less than $1/2^t$, or in other words $\Pr(Y_t|X') < 1/2^t$. How do we turn information about $\Pr(Y_t|X')$ into information about $\Pr(X'|Y_t)$ or $\Pr(X|Y_t) = 1 - \Pr(X'|Y_t)$? Use Bayes' rule.

Theorem A.1 (Bayes' Rule)**.** *For outcomes A and B,*

$$\Pr(A|B) = \frac{\Pr(B|A)\Pr(A)}{\Pr(B|A)\Pr(A) + \Pr(B|A')\Pr(A')},$$

where A' is the outcome complementary to A.

Proof. On the right side, the numerator is $(\Pr(B \cap A)/\Pr(A))\Pr(A) = \Pr(B \cap A)$, while the denominator is

$$\begin{aligned}(\Pr(B \cap A)/\Pr(A))\Pr(A) + (\Pr(B \cap A')/\Pr(A'))\Pr(A') &= \Pr(B \cap A) + \Pr(B \cap A') \\ &= \Pr(B).\end{aligned}$$

Therefore the right side is $\Pr(B \cap A)/\Pr(B) = \Pr(A|B)$. □

Bayes' rule has real-world counterintuitive consequences for medical tests. If a test for a disease will have a positive result 95% of the time for people with the disease and a negative result 95% of the time for people without the disease, and the disease itself is in only 2% of the population, then Bayes' rule implies that the probability of having the disease if the test result is positive (the initial information told us the probability of the test result being positive if the patient has the disease, a *different* situation) is only about 28%, so if the test comes back positive you're more than twice as likely *not* to have the disease as you are to have it. Googling "Bayes rule false positive" will produce numerous webpages with worked examples of this phenomenon.

We will use Bayes' rule to estimate the "probability" that n is prime if t runs of the Solovay–Strassen test turn up no Euler witnesses for n, which is $\Pr(X|Y_t)$. Corollary 3.2(2) implies $\Pr(Y_t|X') < 1/2^t$, so by Bayes' rule,

$$\Pr(X|Y_t) = \frac{\Pr(Y_t|X)\Pr(X)}{\Pr(Y_t|X)\Pr(X) + \Pr(Y_t|X')\Pr(X')} > \frac{\Pr(Y_t|X)\Pr(X)}{\Pr(Y_t|X)\Pr(X) + \Pr(X')/2^t}. \tag{A.1}$$

What can we say about $\Pr(X)$, $\Pr(X')$, and $\Pr(Y_t|X)$? Of course $\Pr(X') = 1 - \Pr(X)$, so a heuristic for one of $\Pr(X)$ or $\Pr(X')$ gives us the other.

The probability $\Pr(X)$: The prime number theorem says roughly that $|\{\text{primes } \leq n\}| \approx n/\log n$, so the "probability" that n is prime can be taken heuristically to be $(n/\log n)/n = 1/\log n$. So we set $\Pr(X) = 1/\log n$ and $\Pr(X') = 1 - 1/\log n$. Feeding this into (A.1),

$$\Pr(X|Y_t) > \frac{\Pr(Y_t|X)/\log n}{\Pr(Y_t|X)/\log n + (1 - 1/\log n)/2^t}. \tag{A.2}$$

The probability $\Pr(Y_t|X)$: Using the definition of conditional probability as a ratio,

$$\Pr(Y_t|X) = \frac{\Pr(Y_t \cap X)}{\Pr(X)}. \tag{A.3}$$

Recall that X is the event of n being prime. On prime numbers the Solovay–Strassen test will never find an Euler witness, so $X \subset Y_t$. Thus (A.3) becomes

$$\Pr(Y_t|X) = \frac{\Pr(X)}{\Pr(X)} = 1.$$

This says the heuristic probability of t trials turning up no Euler witnesses given that n is prime is 1, which makes sense. Feeding this into (A.2), we get

$$\Pr(X|Y_t) > \frac{1/\log n}{1/\log n + (1 - 1/\log n)/2^t} = \frac{1}{1 + (\log n - 1)/2^t}.$$

We have $1/(1+x) > 1 - x$ if $0 < x < 1$, so if $2^t > \log n$ (which means the number t of tests that we run will have to depend in a weak way on the size of n) then $\Pr(X|Y_t) > 1 - (\log n - 1)/2^t > 1 - (\log n)/2^t$ and thus also $\Pr(X'|Y_t) = 1 - \Pr(X|Y_t) < (\log n)/2^t$.

Theorem A.2. *If $n > 1$ is odd and the Solovay–Strassen test runs t times without finding an Euler witness, and $2^t > \log n$, then n is prime with "probability" $> 1 - (\log n)/2^t$ and n is composite with "probability" $< (\log n)/2^t$.*

At the start of this section we said n is prime with "probability" greater than $1 - 1/2^t$ if t tests don't produce an Euler witness. A better heuristic probability, accounting for Bayes' rule, requires $2^t > \log n$ and the effect is to multiply $1/2^t$ by $\log n$ in the probabilities.

How does the condition $2^t > \log n$ look in Example 3.7 when n is the 54-digit number in (3.1)? We want $t > \log_2(\log n) \approx 6.93$, so if $t \geq 7$ and t trials of the Solovay–Strassen test are run without an Euler witness being found then the "probability" that n is composite should be changed from at most $1/2^t$ to at most $(\log n)/2^t \approx 122.19/2^t$. Since $122.19/2^{t+7} < 1/2^t$ for any t we only need to increase the number of trials from 100 to 107 for our "Bayes–corrected" heuristic probability in Theorem A.2 to be as small as the "Bayes–uncorrected" heuristic probability we used with 100 trials in Example 3.7.

Since $\log_2(\log n)$ is such a slowly growing function, for practical purposes the required bound $t > \log_2(\log n)$ is a very mild condition for the use of better probabilistic heuristics with Bayes' rule.

References

[1] M. Agrawal, N. Kayal, and N. Saxena, "PRIMES is in P," Annals of Math. **160** (2004), 781–793.
[2] M. M. Artjuhov, "Certain criteria for the primality of numbers connected with the little Fermat theorem" (Russian), Acta Arith. **12** (1967), 355-364.
[3] E. Bach, "Explicit bounds for primality testing and related problems," Math. Comp. **55** (1990), 355–380.

[4] P. Erdos and C. Pomerance, "On the Number of False Witnesses for a Composite Number," Math. of Computation **46** (1986), 259–279.
[5] D. H. Lehmer, "Strong Carmichael Numbers," J. Austral. Math. Soc. **21** (1976), 508–510.
[6] G. L. Miller, "Riemann's Hypothesis and tests for primality," J. Computer and System Sciences **13** (1976), 300–317.
[7] M. O. Rabin, "Probabilistic algorithm for testing primality," J. Number Theory **12** (1980), 128–138.
[8] J. Oesterlé, "Versions effectives du théorème de Chebotarev sous l'hypothése de Riemann généralisée," Astérisque **61** (1979), 165–167.
[9] R. M. Solovay and V. Strassen, "A fast Monte-Carlo test for primality," SIAM Journal on Computing **6** (1977), 84-85.
[10] R. M. Solovay and V. Strassen, "Erratum: A fast Monte-Carlo test for primality," SIAM Journal on Computing **7** (1978), 1.