THE MILLER–RABIN TEST

KEITH CONRAD

1. Introduction

The Miller–Rabin test is the most widely used probabilistic primality test. For odd composite $n > 1$ at least 75% of numbers from to 1 to $n-1$ are witnesses in the Miller–Rabin test for n. We will describe the test and prove the 75% lower bound, which is better than the 50% lower bound for witnesses in the Solovay–Strassen test for n.

2. The Miller–Rabin test

The Fermat and Solovay–Strassen tests are each based on translating a congruence modulo prime numbers, either Fermat's little theorem or Euler's congruence, over to the setting of composite numbers and hoping to make it fail there. The Miller–Rabin test uses a similar idea, but involves a system of congruences.

For an odd integer $n > 1$, factor out the largest power of 2 from $n-1$, say $n-1 = 2^e k$ where $e \geq 1$ and k is odd. This meaning for e and k will be used throughout. The polynomial $x^{n-1} - 1 = x^{2^e k} - 1$ can be factored repeatedly as often as we have powers of 2 in the exponent:

$$\begin{aligned}
x^{2^e k} - 1 &= (x^{2^{e-1}k})^2 - 1 \\
&= (x^{2^{e-1}k} - 1)((x^{2^{e-1}k} + 1) \\
&= (x^{2^{e-2}k} - 1)(x^{2^{e-2}k} + 1)((x^{2^{e-1}k} + 1) \\
&\ \ \vdots \\
&= (x^k - 1)(x^k + 1)(x^{2k} + 1)(x^{4k} + 1)\cdots(x^{2^{e-1}k} + 1).
\end{aligned}$$

If n is prime and $1 \leq a \leq n-1$ then $a^{n-1} - 1 \equiv 0 \bmod n$ by Fermat's little theorem, so using the above factorization we have

$$(a^k - 1)(a^k + 1)(a^{2k} + 1)(a^{4k} + 1)\cdots(a^{2^{e-1}k} + 1) \equiv 0 \bmod n.$$

When n is prime one of these factors must be $0 \bmod n$, so

$$a^k \equiv 1 \bmod n \text{ or } a^{2^i k} \equiv -1 \bmod n \text{ for some } i \in \{0, \ldots, e-1\}. \tag{2.1}$$

Example 2.1. If $n = 13$ then $n - 1 = 4 \cdot 3$, so $e = 2$, $k = 3$, and (2.1) says $a^3 \equiv 1 \bmod n$ or $a^3 \equiv -1 \bmod n$ or $a^6 \equiv -1 \bmod n$ for each a from 1 to 12.

Example 2.2. If $n = 41$ then $n - 1 = 8 \cdot 5$, so $e = 3$, $k = 5$, and (2.1) says $a^7 \equiv 1 \bmod n$ or one of a^5, a^{10}, or a^{20} is congruent to $-1 \bmod n$ for each a from 1 to 40.

If n is not prime the congruences in (2.1) still make sense, but they might all be false for many a in $\{1, \ldots, n-1\}$, and this will lead to a primality test.

Definition 2.3. For odd $n > 1$, write $n-1 = 2^e k$ with k odd and pick $a \in \{1, \ldots, n-1\}$. We say a is a *Miller–Rabin witness* for n if all of the congruences in (2.1) are false:

$$a^k \not\equiv 1 \bmod n \textbf{ and } a^{2^i k} \not\equiv -1 \bmod n \textbf{ for all } i \in \{0, \ldots, e-1\}.$$

We say a is a *Miller–Rabin nonwitness* for n (and n is called a *strong pseudoprime* to the base a) if one of the congruences in (2.1) is true:

$$a^k \equiv 1 \bmod n \textbf{ or } a^{2^i k} \equiv -1 \bmod n \textbf{ for some } i \in \{0, \ldots, e-1\}.$$

As in the Fermat and Solovay–Strassen tests, we are using the term "witness" to mean a number that proves n is composite. An odd prime has no Miller–Rabin witnesses, so when n has a Miller–Rabin witness it must be composite.

In the definition of a Miller–Rabin witness, the case $i = 0$ says $a^k \not\equiv -1 \bmod n$, so another way of describing a witness is $a^k \not\equiv \pm 1 \bmod n$ and $a^{2^i k} \not\equiv -1 \bmod n$ for all $i \in \{1, \ldots, e-1\}$, where this range of values for i is empty if $e = 1$ (that is, if $n \equiv 3 \bmod 4$).

Example 2.4. If $n \equiv 3 \bmod 4$ then $e = 1$ (and conversely). In this case $k = (n-1)/2$, so a is a Miller–Rabin witness for n if $a^{(n-1)/2} \not\equiv \pm 1 \bmod n$, while a is a Miller–Rabin nonwitness for n if $a^{(n-1)/2} \equiv \pm 1 \bmod n$.

Miller–Rabin witnesses and nonwitnesses can also be described using the list of powers

$$(a^k, a^{2k}, a^{4k}, \ldots, a^{2^{e-1}k}) = (\{a^{2^i k}\})_{i=0}^{e-1} \tag{2.2}$$

with all terms considered mod n. We call this the *Miller–Rabin sequence* for n that is generated by a. For example, to write a Miller–Rabin sequence for $n = 57$ write $57 - 1 = 2^3 \cdot 7$. Since $e = 3$ and $k = 7$, the Miller–Rabin sequence for 57 that is generated by a is (a^7, a^{14}, a^{28}). Each term in a Miller–Rabin sequence is the square of the previous term, so if 1 occurs in the sequence then all later terms are 1. If -1 occurs in the sequence then all later terms are also 1. Thus -1 can occur *at most once* in this sequence. If $1 \le a \le n-1$ then a is a Miller–Rabin nonwitness for n if and only if (2.2) looks like

$$(1, \ldots) \bmod n \quad \text{or} \quad (\ldots, -1, \ldots) \bmod n$$

and a is a Miller–Rabin witness for n if and only if (2.2) is anything else: the first term is not 1 (equivalently, the terms in the Miller–Rabin sequence are not all 1) and there is no -1 anywhere in (2.2).

Example 2.5. Let $n = 9$. Since $n - 1 = 8 = 2^3$, $e = 3$ and $k = 1$. The Miller–Rabin sequence for 9 generated by a is $(a, a^2, a^4) \bmod 9$. In the table below we list this sequence for $a = 1, 2, \ldots, 8$. The Miller–Rabin witnesses are 2, 3, 4, 5, 6, and 7, so the proportion of Miller–Rabin witnesses is $6/8 = 3/4$.

$a \bmod 9$	1	2	3	4	5	6	7	8
$a^2 \bmod 9$	1	4	0	7	7	0	4	1
$a^4 \bmod 9$	1	7	0	4	4	0	7	1

Example 2.6. Let $n = 29341$. Since $n - 1 = 2^2 \cdot 7335$, the Miller–Rabin sequence for n generated by a is $(a^k, a^{2k}) \bmod n$ where $k = 7335$. When $a = 2$, the Miller–Rabin sequence is $(26424, 29340)$. The last term is $-1 \bmod n$, so -1 appears and therefore 2 is not a Miller–Rabin witness for n. When $a = 3$ the Miller–Rabin sequence is $(22569, 1)$. The first term is not 1 and no term is -1, so 3 is a Miller–Rabin witness for n and thus n is composite.

Example 2.7. Let $n = 30121$. Since $n - 1 = 2^3 \cdot 3765$, the Miller–Rabin sequence for n generated by a is $(a^k, a^{2k}, a^{4k}) \bmod n$ where $k = 3765$. When $a = 2$, this sequence is (15036,73657, 39898,1,1). The first term is not 1 and no term is $-1 \bmod n$, so 2 is a Miller–Rabin witness for n.

Example 2.8. Let $n = 75361$. Since $n - 1 = 2^5 \cdot 2355$, the Miller–Rabin sequence for n generated by a is $(a^k, a^{2k}, a^{4k}, a^{8k}, a^{16k}) \bmod n$ where $k = 2355$. When $a = 2$, this sequence is (330, 18537,1). The first term is not 1 and there is no $-1 \bmod n$, so 2 is a Miller–Rabin witness for n.

The first odd composite number not having 2 or 3 as an Euler witness is 1729, while the first odd composite number not having 2 or 3 as a Miller–Rabin witness is $n = 1373653$. Since $n-1 = 2^2 \cdot 343413$, a Miller–Rabin sequence for n is $(a^k, a^{2k}) \bmod n$ where $k = 343413$. The Miller–Rabin sequence generated by 2 is $(890592, 137652)$, with the last term being $-1 \bmod n$, and the Miller–Rabin sequence generated by 3 is $(1, 1)$. The number 5 is a Miller–Rabin witness for n: it generates the Miller–Rabin sequence (1199564, 73782). An exhaustive computer search has shown that every odd positive composite number less than 10^{10} has 2, 3, 5, or 7 as a Miller–Rabin witness except for 3215031751, and 11 is a Miller–Rabin witness for that number.

There is a more intuitive way to think about Miller–Rabin witnesses. If n is an odd prime the congruence $a^{n-1} \equiv 1 \bmod n$ from Fermat's little theorem can be rewritten as $(a^k)^{2^e} \equiv 1 \bmod n$, so $a^k \bmod n$ has order equal to a power of 2 that is at most 2^e. Therefore if $a^k \not\equiv 1 \bmod n$ the order of $a^k \bmod n$ is 2^j for some $j \in \{1, \ldots, e\}$, so $x := a^{2^{j-1}k} \bmod n$ has $x^2 \equiv 1 \bmod n$ and $x \not\equiv 1 \bmod n$. The only square roots of unity modulo an odd prime are $\pm 1 \bmod n$, so if $a^k \not\equiv 1 \bmod n$ and none of the numbers $a, a^2, a^4, \ldots, a^{2^{e-1}k}$ is $-1 \bmod n$ then we have a contradiction: n can't be prime. We have rediscovered the definition of a Miller–Rabin nonwitness, and it shows us that *the idea behind Miller–Rabin witnesses is to find an unexpected square root of* $1 \bmod n$. This is not always what we actually find, since the premise $a^{n-1} \equiv 1 \bmod n$ for prime n might not actually be true for composite n. In Example 2.5, for instance, no Miller–Rabin witness for 9 is a square root of 1 mod 9.

Euler witnesses are always Miller–Rabin witnesses (Theorem 6.1), and sometimes they are the same set of numbers (Corollary 6.2), but when there are more Miller–Rabin witnesses than Euler witnesses there can be a lot more. This is not very impressive for $n = 30121$, whose proportion of Euler witnesses is an already high 96.4% and its proportion of Miller–Rabin witnesses is 99.1%. But for $n = 75361$, the proportion of Euler witnesses is 61.7% while the proportion of Miller–Rabin witnesses is a much higher 99.4%.

The next theorem quantifies at least how large the proportion of Miller–Rabin witnesses is for odd composite numbers.

Theorem 2.9. *Let $n > 1$ be odd and composite.*

The proportion of integers from 1 to $n-1$ that are Miller–Rabin witnesses for n is greater than 75% except at $n = 9$, where the proportion is 75%.

Equivalently, the proportion of integers from 1 to $n-1$ that are Miller–Rabin nonwitnesses for n is less than 25% except at $n = 9$, where the proportion is 25%.

Theorem 2.9, due independently to Miller [9] and Monier [8], will be proved in Section 5. The proof is complicated, so first in Section 4 we will prove in a simpler way that the proportion of Miller–Rabin witnesses is greater than 50%, and the ideas in that proof will be useful for us when we later show the bound is at least 75%. We saw in Example 2.5 that the 75% lower bound is reached for $n = 9$, and as an asymptotic lower bound it is probably sharp: if p and $2p - 1$ are prime and $p \equiv 3 \bmod 4$ then Monier [8, p. 102] showed the proportion of Miller–Rabin witnesses for $p(2p-1)$ tends to 75% if we can let $p \to \infty$, and it's expected that we can: it is conjectured that p and $2p-1$ are both prime for infinitely many primes $p \equiv 3 \bmod 4$.

Example 2.10. For the prime $p = 79$, $2p - 1 = 157$ is also prime and the proportion of Miller–Rabin witnesses for $p(2p - 1) = 12403$ is $9360/12402 \approx 75.4\%$.

Here is the **Miller–Rabin test** for deciding if an odd $n > 1$ is prime. In the last step we appeal to the bound in Theorem 2.9.

(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 a is a Miller–Rabin witness for n then stop the test and declare (correctly) "n is composite."
(4) If a is not a Miller–Rabin witness for n then go to step 2 and pick another random a from 1 to $n - 1$.
(5) If the test runs for t trials without terminating then say "n is prime with probability at least $1 - 1/4^t$."

(A better probabilistic heuristic in the last step, using Bayes' rule, should use the lower bound $1 - (\log n)/4^t$ and we need to pick t at the start so that $4^t > \log n$.)

If we believe the Generalized Riemann Hypothesis (GRH), which is one of the most important unsolved problems in mathematics, then the Miller–Rabin test can be converted from a probabilistic primality test into a deterministic primality test that runs in polynomial time: Bach [3] showed GRH implies that some Miller–Rabin witness for n is at most $2(\log n)^2$ if n has any Miller–Rabin witnesses at all. Historically things were reversed: Miller introduced "Miller's test" in a deterministic form assuming GRH,[1] and a few years later Rabin proved Theorem 2.9 to make the method of Miller's test no longer dependent on any unproved hypotheses if it is treated as a probabilistic test. This became the Miller–Rabin test. We will discuss its history further in Section 7.

3. Multiplication of Miller–Rabin nonwitnesses

Here are descriptions of nonwitnesses for the Fermat test, Solovay–Strassen test, and Miller–Rabin test. For odd $n > 1$ and $1 \leq a \leq n - 1$,

(i) a is a Fermat nonwitness for n when

$$a^{n-1} \equiv 1 \bmod n,$$

(ii) a is an Euler nonwitness for n when

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

and

(iii) a is a Miller–Rabin nonwitness for n when

$$a^k \equiv 1 \bmod n \text{ or } a^{2^i k} \equiv -1 \bmod n \text{ for some } i \in \{0, \dots, e-1\}.$$

In all three cases, 1 and $n-1$ are nonwitnesses (note n is odd). Another common feature is that all three types of nonwitnesses are relatively prime to n. It is easy to see that the

[1]Miller did not rely on Bach's work involving GRH, which had not yet appeared. He relied instead on similar but less precise consequences of GRH due to Ankeny.

Fermat nonwitnesses and Euler nonwitnesses for n each form a *group* under multiplication mod n. If n is composite then the Euler nonwitnesses for n are a proper subgroup of the invertible numbers mod n, and this is also true for the Fermat witnesses for n if n is not a Carmichael number. That is why the proportions of Fermat nonwitnesses (for non-Carmichael n) and Euler nonwitnesses are each less than 50% when n is composite, which makes the proportions of Fermat witnesses and Euler witnesses each greater than 50%.

The set of Miller–Rabin nonwitnesses is often *not* a group under multiplication mod n: the product of two Miller–Rabin nonwitnesses for n could be a witness. (Since 1 is a Miller–Rabin nonwitness for any n and the multiplicative inverse mod n of a Miller–Rabin nonwitness for n is a Miller–Rabin nonwitness for n, the only reason the nonwitnesses might not be a group has to be failure of closure under multiplication.)

Example 3.1. The Miller–Rabin nonwitnesses for 65 are 1, 8, 18, 47, 57, and 64. Modulo 65 we have $8 \cdot 18 = 14$ but 14 is a Miller–Rabin witness for 65. The Miller–Rabin sequences for 65 generated by 8 and 18 are $(8, 64, 1, 1, 1, 1)$ and $(18, 64, 1, 1, 1, 1)$, which each include $-1 \bmod 65$ in the second position, while the sequence generated by 14 is $(14, 1, 1, 1, 1, 1)$, which does not start with 1 or include -1 anywhere.

Example 3.2. The Miller–Rabin nonwitnesses for 85 are 1, 13, 38, 47, 72, 84, but modulo 85 we have $13 \cdot 38 = 69$ and 69 is a Miller–Rabin witness for 85.

We can understand why the Miller–Rabin nonwitnesses for n might not be a group under multiplication mod n by thinking about how the different conditions for being a nonwitness interact under multiplication. First of all, if $n \equiv 3 \bmod 4$ then the Miller–Rabin witnesses for n are the solutions to $a^k \equiv \pm 1 \bmod n$ (Example 2.4), which is a group. If $n \equiv 1 \bmod 4$ (so $e \geq 2$) and a and b are Miller–Rabin nonwitnesses for n then this could happen in three ways (up to the ordering of a and b):

(i) $a^k \equiv \pm 1 \bmod n$ and $b^k \equiv \pm 1 \bmod n$
(ii) $a^{2^i k} \equiv -1 \bmod n$ for some i from 1 to $e-1$ and $b^k \equiv \pm 1 \bmod n$
(ii) $a^{2^i k} \equiv -1 \bmod n$ and $b^{2^{i'} k} \equiv \pm 1 \bmod n$ for some i and i' from 1 to $e-1$.

In the first case $(ab)^k \equiv \pm 1 \bmod n$, so $ab \bmod n$ is a Miller–Rabin nonwitness for n. In the second case $b^{2^i k} \equiv 1 \bmod n$ since $i > 0$, so $(ab)^{2^i k} \equiv -1 \bmod n$ and again $ab \bmod n$ is a Miller–Rabin nonwitness for n. In the third case $ab \bmod n$ is a nonwitness if $i \neq i'$ for a reason similar to the second case, but there is a potential problem when $i = i'$ since $(ab)^{2^i k} \equiv (-1)(-1) \equiv 1 \bmod n$ with $i > 0$ and for ab to be a nonwitness for n we have to rely on information about terms in the Miller–Rabin sequence generated by ab before the i-th term. We see this happening in Example 3.1: the Miller–Rabin sequences for 65 generated by 8 and 47 each contain -1 in the second term, which cancel under multiplication, but their first terms don't have product $\pm 1 \bmod 65$.

From this case-by-case analysis, we see that the product of two Miller–Rabin nonwitnesses a and b might not be a nonwitness only if $n \equiv 1 \bmod 4$ and $a^{2^i k} \equiv b^{2^i k} \equiv -1 \bmod n$ for a common choice of i, or in other words when $-1 \bmod n$ occurs in the same position past the first position in the Miller–Rabin sequences generated by a and b.

The following two theorems give different conditions on odd $n > 1$ that guarantee the Miller–Rabin nonwitnesses are a group under multiplication mod n.

Theorem 3.3. *If $-1 \not\equiv \square \bmod n$ then the Miller–Rabin nonwitnesses for n are the solutions to $a^k \equiv \pm 1 \bmod n$, which form a group under multiplication mod n.*

Proof. If $-1 \not\equiv \Box \bmod n$ then the congruence $a^{2^i k} \equiv -1 \bmod n$ has no solution for $i > 0$, so the Miller–Rabin nonwitnesses for n are the $a \in \{1, \ldots, n-1\}$ that satisfy $a^k \equiv \pm 1 \bmod n$. This congruence condition on a clearly defines a group under multiplication mod n. $\square$

A simple case where $-1 \not\equiv \Box \bmod n$ is if $n \equiv 3 \bmod 4$, and here the Miller–Rabin nonwitnesses for n are $\{1 \le a \le n-1 : a^{(n-1)/2} \equiv \pm 1 \bmod n\}$.

Theorem 3.4. *If $n = p^\alpha$ for prime p and $\alpha \ge 1$, the Miller–Rabin nonwitnesses for n are the solutions to $a^{p-1} \equiv 1 \bmod p^\alpha$, which form a group under multiplication mod n.*

We allow $\alpha = 1$, corresponding to n being prime, since the theorem is valid in that case.

Proof. Let $a \in \{1, \ldots, n-1\}$ be a Miller–Rabin nonwitness. Since a is relatively prime to $n = p^\alpha$, Euler's theorem tells us $a^{\varphi(n)} \equiv 1 \bmod n$. At the same time, as a nonwitness we have either $a^k \equiv 1 \bmod n$ or $a^{2^i k} \equiv -1 \bmod n$ for some $i \le e-1$, and both cases imply $a^{2^e k} \equiv 1 \bmod n$, or equivalently $a^{n-1} \equiv 1 \bmod n$. Thus the order of a mod n divides $(\varphi(n), n-1) = (p^{\alpha-1}(p-1), p^\alpha - 1)$. Since p is relatively prime to $p^\alpha - 1$ and $p-1$ divides $p^\alpha - 1$, we have $(p^{\alpha-1}(p-1), p^\alpha - 1) = p-1$, so $a^{p-1} \equiv 1 \bmod p^\alpha$.

Conversely, suppose $a^{p-1} \equiv 1 \bmod p^\alpha$. Write $p - 1 = 2^f \ell$, where $f \ge 1$ and ℓ is odd. Since $p-1$ is a factor of $p^\alpha - 1 = 2^e k$, we have $f \le e$ and $\ell \mid k$. Since $(a^\ell)^{2^f} \equiv 1 \bmod p^\alpha$, the order of $a^\ell \bmod p^\alpha$ is 2^j for some $j \in \{0, \ldots, f\}$.

If $j = 0$, so $a^\ell \equiv 1 \bmod p^\alpha$, then $a^k \equiv 1 \bmod p^\alpha$ as $\ell \mid k$.

If instead $j \ge 1$, then $x := (a^\ell)^{2^{j-1}}$ satisfies $x \not\equiv 1 \bmod p^\ell$ but $x^2 \equiv 1 \bmod p^\ell$. Thus $p^\ell \mid (x+1)(x-1)$ and $x+1$ and $x-1$ differ by 2, so at most one of them can be divisible by p and that number therefore has to absorb the entire factor p^ℓ. In other words, $p^\ell \mid (x+1)$ or $p^\ell \mid (x-1)$, so $x \equiv \pm 1 \bmod p^\ell$.[2] Since $x \not\equiv 1 \bmod p^\ell$, we get $x \equiv -1 \bmod p^\ell$. Recalling what x is, $a^{2^{j-1}\ell} \equiv -1 \bmod p^\alpha$. Since $\ell \mid k$ and k is odd, raising both sides to the k/ℓ power gives us $a^{2^i k} \equiv -1 \bmod p^\alpha$ where $i = j - 1 \in \{0, \ldots, f-1\} \subset \{0, \ldots, e-1\}$. $\square$

The sufficient conditions in Theorems 3.3 and 3.4 turn out to be necessary too: for odd $n > 1$ such that $-1 \equiv \Box \bmod n$ and n has at least two different prime factors, the Miller–Rabin nonwitnesses for n do not form a group under multiplication. We omit a proof.

Although the Miller–Rabin nonwitnesses for an odd composite $n > 1$ are not always a group under multiplication mod n, they are always in a proper subgroup of the invertible numbers mod n, as we will see in Sections 4 and 5. This allows work on the Generalized Riemann Hypothesis (GRH) as described at the end of Section 3 to be applied: if GRH is true then any odd composite $n > 1$ has a Miller–Rabin witness $\le 2(\log n)^2$, so the truth of GRH would imply the Miller–Rabin test is deterministic in polynomial time.

4. Proving the proportion of Miller–Rabin witnesses is over 50%

The proof of the 75% lower bound for the proportion of Miller–Rabin witnesses for an odd composite $n > 1$ (Theorem 2.9) is not easy. It is much easier to prove the proportion is over 50%[3] so we present this argument here first.

[2]What we just proved, that the only solutions to $x^2 = 1$ modulo an odd prime power are ± 1, will be used again in our proof of Theorem 2.9. It is *false* for powers of 2 starting with 8: modulo 2^α for any $\alpha \ge 3$ there are 4 square roots of unity.

[3]We will see in Section 6 that every Euler witness is a Miller–Rabin witness, so the 50% lower bound for the proportion of Miller–Rabin witnesses also follows from the 50% lower bound for the proportion of Euler witnesses, but a proof that way is harder.

Theorem 4.1. *If $n > 1$ is odd and composite then the proportion of Miller–Rabin witnesses for n is more than 50%. That is, more than 50% of $a \in \{1, \dots, n-1\}$ satisfy $a^k \not\equiv 1 \bmod n$ and $a^{2^i k} \not\equiv -1 \bmod n$ for all $i \in \{0, \dots, e-1\}$.*

Proof. We will show the proportion of Miller–Rabin *nonwitnesses* for n is less than 50% by showing they are contained in a proper subgroup of the invertible numbers mod n. Since a proper subgroup of a group is at most half the size of the group, the set of Miller–Rabin witnesses for n in $\{1, \dots, n-1\}$ includes at least half the invertible numbers mod n and all the noninvertible numbers mod n in $\{1, \dots, n-1\}$ (there are noninvertible numbers mod n, as n is composite). Thus the proportion of Miller–Rabin witnesses for n is over 50%.

We take cases if n is a prime power or not a prime power.

Case 1: n is a prime power. Write $n = p^\alpha$ where p is an odd prime and $\alpha \geq 2$. By Theorem 3.4, the Miller–Rabin nonwitnesses for n are the solutions in $\{1, \dots, n-1\}$ to $a^{p-1} \equiv 1 \bmod n$, which are a group under multiplication mod n. The order of such an a divides $p-1$, so it is not divisible by p, and also there are invertible numbers mod n with order divisible by p: an explicit such number is $1+p$, whose order mod p^α is $p^{\alpha-1}$. Therefore the Miller–Rabin nonwitnesses for n form a proper subgroup of the invertible numbers mod n, and we explained at the start of the proof why this is sufficient.

Case 2: n is not a prime power. Let $i_0 \in \{0, \dots, e-1\}$ be maximal such that some $a_0 \in \mathbf{Z}$ satisfies $a_0^{2^{i_0}} \equiv -1 \bmod n$. (Since $(-1)^{2^0} = -1$ there is an i_0, and a_0 is automatically relatively prime to n.)

The set

$$G_n = \{1 \leq a \leq n-1 : a^{2^{i_0} k} \equiv \pm 1 \bmod n\}$$

is a group under multiplication modulo n and contains every a satisfying one of the conditions

(1) $a^k \equiv 1 \bmod n$,
(2) $a^{2^i k} \equiv -1 \bmod n$ for some $i \in \{0, \dots, e-1\}$.

If $a^k \equiv 1 \bmod n$, then $a^{2^{i_0} k} \equiv 1 \bmod n$. If $a^{2^i k} \equiv -1 \bmod n$ for some i from 0 to $e-1$, then $(a^k)^{2^i} \equiv -1 \bmod n$, so $i \leq i_0$ by the maximality of i_0, and thus $a^{2^{i_0} k} \equiv -1 \bmod n$ if $i = i_0$ and $a^{2^{i_0} k} \equiv 1 \bmod n$ if $i < i_0$. Thus each a in $\{1, \dots, n-1\}$ that satisfies (1) or (2) is in G_n.

We will show G_n is a proper subgroup of the invertible numbers mod n. Let p be a prime factor of n and write $n = p^\alpha n'$ where $\alpha \geq 1$ and n' is not divisible by p. Both p^α and n' are odd and not 1 (because n is not a prime power), so each is at least 3.

By the Chinese remainder theorem, some $a \in \{1, \dots, n-1\}$ satisfies the two congruences

$$a \equiv a_0 \bmod p^\alpha, \quad a \equiv 1 \bmod n'.$$

Since $(a_0, n) = 1$ we get $(a, n) = 1$. Working modulo p^α and then modulo n',

$$a^{2^{i_0} k} \equiv a_0^{2^{i_0} k} \equiv (-1)^k \equiv -1 \bmod p^\alpha \Longrightarrow a^{2^{i_0} k} \not\equiv 1 \bmod n$$

since $-1 \not\equiv 1 \bmod p^\alpha$, and

$$a^{2^{i_0} k} \equiv 1 \bmod n' \Longrightarrow a^{2^{i_0} k} \not\equiv -1 \bmod n$$

since $-1 \not\equiv 1 \bmod n'$. Thus $a^{2^{i_0} k} \not\equiv \pm 1 \bmod n$, so $(a, n) = 1$ and $a \notin G_n$. $\square$

An alternate proof of Theorem 4.1, taking cases if n is or is not a Carmichael number rather than if n is or is not a prime power, is in [5, Section 5.3]. Our proof of Theorem 4.1 is a modification of the argument given there.

The proof of Case 1 used Theorem 3.4, which relied on the interplay between the congruences $a^{n-1} \equiv 1 \bmod n$ and $a^{\varphi(n)} \equiv 1 \bmod n$ when n is a prime power. The proof of Case 2, on the other hand, did not involve Euler's theorem for modulus n and in fact did not really need e and k to come from a factorization of $n-1$ at all: the reasoning from Case 2 proves the following result.

Corollary 4.2. *Let $e, k \geq 1$ with k odd. If $n > 1$ is odd and not a prime power, more than 50% of $a \in \{1, \ldots, n-1\}$ satisfy $a^k \not\equiv 1 \bmod n$ and $a^{2^i k} \not\equiv -1 \bmod n$ for all $i \in \{0, \ldots, e-1\}$.*

Proof. The proof of Case 2 of Theorem 4.1 carries over to this setting. We don't need $2^e k$ to be $n-1$. Details are left for the reader to check. □

In the appendix (Section A) we will use Corollary 4.2 to develop a probabilistic factorization algorithm.

Corollary 4.2 is invalid when n is an odd prime power: if $n = p^\alpha$ for an odd prime p and we choose e and k by $2^e k = \varphi(n)$ then the only $a \in \{1, \ldots, n-1\}$ satisfying $a^k \not\equiv 1 \bmod n$ and $a^{2^i k} \not\equiv -1 \bmod n$ for all $i \in \{0, \ldots, e-1\}$ are the a not relatively prime to n (this is because modulo p^α the only element of order 2 is -1), and the proportion of such a is

$$1 - \frac{\varphi(n)}{n-1} = 1 - \frac{p^\alpha(1-1/p)}{p^\alpha - 1} < 1 - \left(1 - \frac{1}{p}\right) = \frac{1}{p},$$

which is less than 50%. This does not contradict Theorem 4.1, which allows n to be a prime power, since the e and k used there are chosen from a factorization of $n-1$, not $\varphi(n)$.

5. Proving the proportion of Miller–Rabin witnesses is at least 75%

In this section we will prove Theorem 2.9. Rather than prove the proportion of Miller–Rabin witnesses for an odd composite $n > 1$ has a lower bound of 75%, with the bound achieved only at $n = 9$, we'll prove the proportion of Miller–Rabin nonwitnesses has an upper bound of 25%, with the bound achieved only at $n = 9$. It is more difficult to prove results about Miller–Rabin nonwitnesses compared to Fermat nonwitnesses or Solovay–Strassen nonwitnesses because the set of Miller–Rabin nonwitnesses is not generally closed under multiplication.

First we will deal with the case that $n = p^\alpha$ is a power of an odd prime and $\alpha \geq 2$. By Theorem 3.4, the Miller–Rabin nonwitnesses for p^α are the solutions to $a^{p-1} \equiv 1 \bmod p^\alpha$. Such a are closed under multiplication mod p^α, which is great (and not true of Miller–Rabin nonwitnesses for general n). How many such a are there from 1 to $p^\alpha - 1$?

In the table below are solutions to $a^{p-1} \equiv 1 \bmod p^\alpha$ when $p = 5$ and 7 with α small. We include $\alpha = 1$.

α	Solutions to $a^4 \equiv 1 \bmod 5^\alpha$	Solutions to $a^6 \equiv 1 \bmod 7^\alpha$
1	1, 2, 3, 4	1, 2, 3, 4, 5, 6
2	1, 7, 18, 24	1, 18, 19, 30, 31, 48
3	1, 57, 68, 124	1, 18, 19, 324, 325, 342
4	1, 182, 443, 624	1, 1047, 1048, 1353, 1354, 2400

This suggests $a^{p-1} \equiv 1 \bmod p^\alpha$ has $p-1$ solutions mod p^α for each α. This is true when $\alpha = 1$ by Fermat's little theorem. For larger α we use induction: if $a^{p-1} \equiv 1 \bmod p^\alpha$ there is a unique $a' \bmod p^{\alpha+1}$ such that $a'^{p-1} \equiv 1 \bmod p^{\alpha+1}$ and $a' \equiv a \bmod p^\alpha$: saying $a' \equiv a \bmod p^\alpha$ is the same as $a' \equiv a + cp^\alpha \bmod p^{\alpha+1}$, with c well-defined mod p, so we want to prove there is a unique choice of $c \bmod p$ making $(a + cp^\alpha)^{p-1} \equiv 1 \bmod p^{\alpha+1}$.

Using the binomial theorem,

$$(a + cp^\alpha)^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}cp^\alpha \bmod p^{\alpha+1},$$

where higher-order terms vanish since $p^{r\alpha} \equiv 0 \bmod p^{\alpha+1}$ for $r \geq 2$. Since $a^{p-1} \equiv 1 \bmod p^\alpha$ we can write $a^{p-1} = 1 + p^\alpha N$ for some $N \in \mathbf{Z}$, so we want to find c that makes

$$(1 + p^\alpha N) + (p-1)a^{p-2}cp^\alpha \equiv 1 \bmod p^{\alpha+1},$$

which is equivalent to

$$N - a^{p-2}c \equiv 0 \bmod p,$$

and this has a unique solution for $c \bmod p$ since $a \bmod p$ is invertible.

Having shown that there are $p-1$ Miller–Rabin nonwitnesses mod p^α, their density is

$$\frac{p-1}{p^\alpha - 1} = \frac{1}{1 + p + \cdots + p^{\alpha-1}}. \tag{5.1}$$

Since $\alpha \geq 2$, this ratio is at most $1/(1+p)$, which in turn is at most $1/(1+3) = 1/4$, and the only way (5.1) equals $1/4$ is if $\alpha = 2$ and $p = 3$, *i.e.*, $n = 3^2 = 9$. For any other p^α the value of (5.1) is less than $1/4$, while for $p^\alpha = 9$ the density is $1/4$ (as we saw explicitly in Example 2.5).

From now on let n have at least two different prime factors. Write, as usual, $n - 1 = 2^e k$ with $e \geq 1$ and k odd.

Let i_0 be the largest integer in $\{0, 1, \ldots, e-1\}$ such that some integer a_0 satisfies $(a_0, n) = 1$ and $a_0^{2^{i_0}} \equiv -1 \bmod n$. By the proof of Case 2 of Theorem 4.1, $i_0 \geq 0$ and the set

$$G_n = \{1 \leq a \leq n-1 : a^{2^{i_0}k} \equiv \pm 1 \bmod n\}$$

is a group under multiplication modulo n that contains every Miller–Rabin nonwitness for n and is a proper subgroup of all invertible numbers mod n.

The ratio $\varphi(n)/|G_n|$ is an integer, and $\varphi(n) < n - 1$ since n is not prime. We will show, when n is not a prime power, that $\varphi(n)/|G_n| \geq 4$, so

$$\text{proportion of Miller–Rabin nonwitnesses for } n = \frac{|\{\text{MR nonwitnesses for } n\}|}{n-1} < \frac{|G_n|}{\varphi(n)} \leq \frac{1}{4}.$$

First we show every $a \in G_n$ satisfies $a^{n-1} \equiv 1 \bmod n$. Since $i_0 \leq e - 1$, the product $2^{i_0+1}k$ divides $2^e k = n - 1$. Each a in G_n satisfies $a^{2^{i_0}k} \equiv \pm 1 \bmod n$, so squaring gives us $a^{2^{i_0+1}k} \equiv 1 \bmod n$. Thus $a^{n-1} \equiv 1 \bmod n$.

A Carmichael number has at least three different prime factors, so either n is not a Carmichael number or it has at least three different prime factors.

<u>Case 1</u>: n is not a Carmichael number.
Set

$$F_n = \{1 \leq a \leq n-1 : a^{n-1} \equiv 1 \bmod n\}.$$

Then

$$\{1 \leq a \leq n-1 : (a, n) = 1\} \supset F_n \supset G_n \tag{5.2}$$

and all three sets are groups under multiplication mod n. We will show both containments in (5.2) are strict, so by group theory $\varphi(n)/|F_n| \geq 2$ and $|F_n|/|G_n| \geq 2$. Thus

$$\frac{\varphi(n)}{|G_n|} = \frac{\varphi(n)}{|F_n|}\frac{|F_n|}{|G_n|} \geq 2 \cdot 2 = 4.$$

If n is not a Carmichael number then some integer relatively prime to n is not in F_n, so the first containment in (5.2) is strict. To show the second containment is strict (that is, $F_n \neq G_n$), pick a prime factor p of n and write $n = p^\alpha n'$ where $\alpha \geq 1$ and p does not divide n', so $n' > 1$. The integer $a \in \{1, \ldots, n-1\}$ constructed in Case 2 of the proof of Theorem 4.1 is not in G_n, and that proof also shows $a \in F_n$: from $a^{2^{i_0}k} \equiv -1 \bmod p^\alpha$ and $a^{2^{i_0}k} \equiv 1 \bmod n'$ we get $a^{2^{i_0+1}k} \equiv 1 \bmod n$ since that congruence is true modulo p^α and modulo n'. Therefore $a^{n-1} \equiv 1 \bmod n$, since $2^{i_0+1}k$ is a factor of $n-1$.

<u>Case 2</u>: n has at least three different prime factors.

Write the prime decomposition of n as $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ for distinct primes p_ℓ, exponents $\alpha_\ell \geq 1$, and $r \geq 3$. Set

$$H_n = \{1 \leq a \leq n-1 : a^{2^{i_0}k} \equiv \pm 1 \bmod p_\ell^{\alpha_\ell} \text{ for } \ell = 1, \ldots, r\}.$$

Then

$$\{1 \leq a \leq n-1 : (a,n) = 1\} \supset H_n \supset G_n \tag{5.3}$$

We will show $|H_n|/|G_n| \geq 4$, so

$$\frac{\varphi(n)}{|G_n|} = \frac{\varphi(n)}{|H_n|}\frac{|H_n|}{|G_n|} \geq \frac{|H_n|}{|G_n|} \geq 4.$$

For integers x and y,

$$x \equiv y \bmod n \Longleftrightarrow x \equiv y \bmod p_\ell^{\alpha_\ell} \text{ for } \ell = 1, \ldots, r.$$

The mapping between groups $f \colon H_n \to \prod_{\ell=1}^r \{\pm 1 \bmod p_\ell^{\alpha_\ell}\}$ that is defined by

$$f(a \bmod n) = (\ldots, a^{2^{i_0}k} \bmod p_\ell^{\alpha_\ell}, \ldots)_{\ell=1}^r$$

is a homomorphism. Set $K_n = \ker f$, so $H_n \supset G_n \supset K_n$. The target group for f has order 2^r. Let's prove f is surjective. It suffices, since f is a homomorphism, to show each r-tuple $(\ldots, 1, -1, 1, \ldots)$ with -1 in one component and 1 in all the other components is in the image of f. By symmetry it's enough to show $(-1, 1, 1, \ldots, 1)$ is in the image of f. That is, we seek an $a \in H_n$ such that

$$a^{2^{i_0}k} \equiv \begin{cases} -1 \bmod p_1^{\alpha_1}, \\ \ \ 1 \bmod p_\ell^{\alpha_\ell}, \text{ if } \ell \geq 2. \end{cases}$$

By the definition of i_0, there is an integer a_0 such that $a_0^{2^{i_0}} \equiv -1 \bmod n$. From the Chinese remainder theorem there is an $a \in \{1, \ldots, n-1\}$ such that

$$a \equiv a_0 \bmod p_1^{\alpha_1}, \quad a \equiv 1 \bmod p_\ell^{\alpha_\ell} \text{ for } \ell \geq 2.$$

Then

$$a^{2^{i_0}k} \equiv a_0^{2^{i_0}k} \equiv (-1)^k \equiv -1 \bmod p_1^{\alpha_1}$$

and

$$a^{2^{i_0}k} \equiv 1 \bmod p_\ell^{\alpha_\ell} \text{ for } \ell \geq 2.$$

Then $f(a \bmod n) = (-1, 1, \ldots, 1)$.

The image $f(H_n)$ has order 2^r. The image $f(G_n)$ is $\{(1, 1, \ldots, 1), (-1, -1, \ldots, -1)\}$, of order 2. Therefore $|H_n|/|K_n| = 2^r$ and $|G_n|/|K_n| = 2$, so $|H_n|/|G_n| = 2^{r-1}$, which is at least 4 since $r \geq 3$.

Our proof of Theorem 2.9 is now complete.

Corollary 5.1. *For odd composite $n > 1$, the Miller–Rabin nonwitnesses for n lie in a proper subgroup of the invertible numbers modulo n.*

Proof. If $n = p^\alpha$ with $\alpha \geq 2$ then the Miller–Rabin nonwitnesses for n are a group of order $p-1$, while $\varphi(p^\alpha) = p^{\alpha-1}(p-1) > p-1$.

If n has $r \geq 2$ different prime factors then the Miller–Rabin nonwitnesses for n lie in G_n. We showed G_n is a proper subgroup of F_n if n is not a Carmichael number, and it's a proper subgroup of H_n if $r \geq 3$. □

Gashkov [6] gave another proof of Theorem 2.9. His strategy is to work more directly with the set S of Miller–Rabin nonwitnesses and find three Miller–Rabin *witnesses* for n, say a, b, and c, that are all invertible numbers mod n such that the sets S, aS, bS, and cS are pairwise disjoint. Verifying the pairwise disjointness is slightly tedious because S is not a group. In any case, all four sets lie in the invertible numbers mod n and have the same size, so pairwise disjointness implies $4|S| \leq \varphi(n) < n-1$, and thus $|S|/(n-1) < 1/4$. Gashkov's argument does not work when n is a certain type of multiple of 3, so he assumes in his proof that n is not divisible by 3.

Remark 5.2. In the Miller–Rabin test it is important to look at $a^{2^i k} \bmod n$ for all i from 0 up to $e-1$. If i only runs over a limited range near $e-1$ then there are infinitely many analogues of Carmichael numbers for this weaker test: composite n whose only witnesses for this weaker test have a factor in common with n. See [4].

6. Euler witnesses are Miller–Rabin witnesses

In the next theorem we prove that any witness for n in the Solovay–Strassen test is a witness for n in the Miller–Rabin test. This fact along with the 75% lower bound on the proportion of Miller–Rabin witnesses in Theorem 2.9 compared to the 50% lower bound for witnesses in the Solovay–Strassen test explains why the Miller–Rabin test is used more often in practice than the Solovay–Strassen test. It also helps that the Miller–Rabin test requires less background to follow its steps (no Jacobi symbols).

Theorem 6.1. *For odd $n > 1$, an Euler witness for n is a Miller–Rabin witness for n.*

Proof. Since nonwitnesses are mathematically nicer than witnesses, we will prove the contrapositive: if an integer $a \in \{1, \ldots, n-1\}$ is not a Miller–Rabin witness for n then it is not an Euler witness for n. That is, the property

$$a^k \equiv 1 \bmod n \text{ or } a^{2^i k} \equiv -1 \bmod n \text{ for some } i \in \{0, \ldots, e-1\}$$

implies the property

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

Clearly not being a Miller–Rabin witness implies $(a, n) = 1$. That it also forces the power $a^{(n-1)/2} = a^{2^{e-1}k}$ to be congruent to $(\frac{a}{n}) \bmod n$ is a more delicate matter to explain.

Since $(n-1)/2 = 2^{e-1}k$ is a multiple of $2^i k$, we have $a^{(n-1)/2} \equiv \pm 1 \bmod n$. Why is the sign on the right side equal to $(\frac{a}{n})$? This is the key issue.

<u>Case 1</u>: $e = 1$, or equivalently $n \equiv 3 \bmod 4$. Not being a Miller–Rabin witness in this case is equivalent to $a^k \equiv \pm 1 \bmod n$, which is the same as $a^{(n-1)/2} \equiv \pm 1 \bmod n$. Let $\varepsilon \in \{1, -1\}$ be the number such that $a^{(n-1)/2} \equiv \varepsilon \bmod n$. The Jacobi symbols with denominator n for both sides are equal, so $(\frac{a}{n})^{(n-1)/2} = (\frac{\varepsilon}{n})$. Since $(n-1)/2$ is odd, $(\frac{a}{n})^{(n-1)/2} = (\frac{a}{n})$. Since

$n \equiv 3 \bmod 4$, $(\frac{-1}{n}) = (-1)^{(n-1)/2} = -1$ and trivially $(\frac{1}{n}) = 1$, so $(\frac{\varepsilon}{n}) = \varepsilon$. Thus $(\frac{a}{n}) = \varepsilon$, so $a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n$ and $(a, n) = 1$. That means a is not an Euler witness for n.

Case 2: $e \geq 2$, or equivalently $n \equiv 1 \bmod 4$. This makes $(n-1)/2 = 2^{e-1}k$ an even multiple of $2^i k$ for every $i \in \{0, \ldots, e-2\}$.

If $a^k \equiv 1 \bmod n$ or $a^{2^i k} \equiv -1 \bmod n$ for some $i < e-1$ then $a^{(n-1)/2} = a^{2^{e-1}k} \equiv 1 \bmod n$. If $a^{2^{e-1}k} \equiv -1 \bmod n$ then $a^{(n-1)/2} \equiv -1 \bmod n$. So we want to show when a is not a Miller–Rabin witness that

$$a^k \equiv 1 \bmod n \text{ or } a^{2^i k} \equiv -1 \bmod n \text{ for some } i \in \{0, \ldots, e-2\} \Longrightarrow \left(\frac{a}{n}\right) = 1$$

and

$$a^{(n-1)/2} \equiv -1 \bmod n \Longrightarrow \left(\frac{a}{n}\right) = -1. \tag{6.1}$$

If $a^k \equiv 1 \bmod n$ then forming the Jacobi symbol of both sides gives $(\frac{a}{n})^k = (\frac{1}{n}) = 1$, so $(\frac{a}{n}) = 1$ since k is odd (this is the same argument used in Case 1). The remaining possibility is that $a^{2^i k} \equiv -1 \bmod n$ for some $i \in \{0, \ldots, e-1\}$. Then

$$a^{(n-1)/2} = a^{2^{e-1}k} \equiv \begin{cases} -1 \bmod n, & \text{if } i = e-1, \\ \ \ 1 \bmod n, & \text{if } 0 \leq i \leq e-2. \end{cases}$$

In correspondence with this formula, we will show when $a^{2^i k} \equiv -1 \bmod n$ that

$$\left(\frac{a}{n}\right) = \begin{cases} -1 \bmod n, & \text{if } i = e-1, \\ \ \ 1 \bmod n, & \text{if } 0 \leq i \leq e-2 \end{cases} \tag{6.2}$$

and thus $a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n$.

The Jacobi symbol $(\frac{a}{n})$ is, by definition, the product of the Legendre symbols $(\frac{a}{p})$ as p runs over the primes dividing n, with each $(\frac{a}{p})$ appearing as often as the multiplicity of p in n. We will compute compute each $(\frac{a}{p})$, and the answer will depend on how highly divisible each $p-1$ is by 2.

For each prime p dividing n, write $p - 1 = 2^{v_p} k_p$ where $v_p \geq 1$ and k_p is odd. Since $a^{2^i k} \equiv -1 \bmod n$ implies $(a^k)^{2^i} \equiv -1 \bmod p$, the order of $a^k \bmod p$ is 2^{i+1}. Therefore $2^{i+1} \mid (p-1)$, so $i < v_p$ and

$$p \equiv 1 \bmod 2^{i+1} \tag{6.3}$$

for each prime p dividing n. Remember that $0 \leq i \leq e-1$ and $a^{2^i k} \equiv -1 \bmod n$.

Since $(p-1)/2 = 2^{v_p-1}k_p$, by Euler's congruence $(\frac{a}{p}) \equiv a^{2^{v_p-1}k_p} \bmod p$. Raising both sides to the k-th power (an odd power), we get $(\frac{a}{p}) \equiv a^{(2^i k)(2^{v_p-1-i}k_p)} \equiv (-1)^{2^{v_p-1-i}} \bmod p$. If $i = v_p - 1$ then $2^{v_p-1-i} = 1$, while if $i < v_p - 1$ then 2^{v_p-1-i} is even. Thus

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & \text{if } i = v_p - 1 \ \ (\text{equiv., } v_p = i+1), \\ \ \ 1, & \text{if } i < v_p - 1 \ \ (\text{equiv., } v_p > i+1). \end{cases} \tag{6.4}$$

The congruence (6.3) can be written as $p \equiv 1 + c_p 2^{i+1} \bmod 2^{i+2}$ where $c_p = 0$ or 1, with $c_p = 0$ when $p \equiv 1 \bmod 2^{i+2}$ $(v_p > i+1)$ and $c_p = 1$ when $p \not\equiv 1 \bmod 2^{i+2}$ $(v_p = i+1)$.

Then (6.4) says $(\frac{a}{p}) = (-1)^{c_p}$ for all primes p dividing n. Writing n as a product of primes $p_1 \cdots p_s$, where these primes are not necessarily distinct,[4]

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{s} \left(\frac{a}{p_j}\right) = \prod_{j=1}^{s} (-1)^{c_{p_j}} = (-1)^{\sum c_{p_j}}.$$

Also

$$n = \prod_{j=1}^{s} p_j \equiv \prod_{j=1}^{s} (1 + c_{p_j} 2^{i+1}) \bmod 2^{i+2} \equiv 1 + \left(\sum_{j=1}^{s} c_{p_j}\right) 2^{i+1} \bmod 2^{i+2}.$$

Let $c = \sum_{j=1}^{s} c_{p_j} = |\{j : v_{p_j} = i+1\}|$, so $(\frac{a}{n}) = (-1)^c$ and

$$n \equiv 1 + c2^{i+1} \bmod 2^{i+2}. \tag{6.5}$$

Recall $n - 1 = 2^e k$ with k odd, so (6.5) says $1 + 2^e k \equiv 1 + c2^{i+1} \bmod 2^{i+2}$. Also recall $0 \le i \le e-1$. If $i = e-1$ then $1 + 2^e k \equiv 1 + c2^e \bmod 2^{e+1}$, so $k \equiv c \bmod 2$. Thus c is odd and $(\frac{a}{n}) = (-1)^c = -1$. If $i < e-1$ then $i + 2 \le e$, so $2^e \equiv 0 \bmod 2^{i+2}$. Thus $1 \equiv 1 + c2^{i+1} \bmod 2^{i+2}$, which implies c is even, so $(\frac{a}{n}) = (-1)^c = 1$. We proved (6.2). □

Corollary 6.2. *If $n \equiv 3 \bmod 4$, Euler witnesses and Miller–Rabin witnesses for n coincide.*

Proof. In Case 1 of the proof of Theorem 6.1 we showed when $n \equiv 3 \bmod 4$ that $a^{(n-1)/2} \equiv \pm 1 \bmod n \Longrightarrow (a, n) = 1$ and $a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n$. The converse is obvious. □

The converse of Corollary 6.2 is not true. For example, Euler witnesses and Miller–Rabin witnesses for 21 are the same (every integer from 2 to 19) but $21 \equiv 1 \bmod 4$.

Corollary 6.3. *An odd $n \equiv 1 \bmod 4$ and $a \in \{1, \ldots, n-1\}$ can satisfy $a^{(n-1)/2} \equiv 1 \bmod n$ and $(\frac{a}{n}) = -1$ but never $a^{(n-1)/2} \equiv -1 \bmod n$ and $(\frac{a}{n}) = 1$.*

Proof. With a computer it is easy to generate examples where $a^{(n-1)/2} \equiv 1 \bmod n$ and $(\frac{a}{n}) = -1$, such as the pairs $(a, n) = (8, 21), (10, 33), (22, 105)$, and so on.

The reason it is impossible to have $a^{(n-1)/2} \equiv -1 \bmod n$ and $(\frac{a}{n}) = 1$ is that such an a would be an Euler witness for n (with $i = e - 1 \ge 1$) but not a Miller–Rabin witness for n since a Miller–Rabin sequence with more than one term can't end with $-1 \bmod n$.[5] More directly, look at (6.1). □

Combining these two corollaries, $a^{(n-1)/2} \equiv -1 \bmod n \Longrightarrow (\frac{a}{n}) = -1$ for all odd $n > 1$, while $a^{(n-1)/2} \equiv 1 \bmod n \Longrightarrow (\frac{a}{n}) = 1$ if $n \equiv 3 \bmod 4$ but not generally if $n \equiv 1 \bmod 4$.

7. The original version of the Miller–Rabin test

The Miller–Rabin test was introduced by Miller [7], but not in the form we used. For each a, the steps in Miller's original test were essentially checking if $a^{n-1} \not\equiv 1 \bmod n$ or if $1 < (a^{2^i k} - 1, n) < n$ for some $i \in \{0, \ldots, e-1\}$. Let's say such an a is a "Miller witness" for n. If there is a Miller witness for n then n is composite. Miller showed the Generalized Riemann Hypothesis (GRH) implies any odd composite n has a Miller witness up to some multiple of $(\log n)^2$, so his test is deterministic assuming GRH. A few years later Monier [8]

[4] This differs from the notation $p_1, \ldots$ for prime factors of n in Section 5, where the primes were distinct.

[5] If $a^{(n-1)/2} \equiv 1 \bmod n$ and $(\frac{a}{n}) = -1$, a is an Euler witness for n and thus is a Miller–Rabin witness for n. There is no contradiction because a Miller–Rabin sequence can have 1 as its last term.

and Rabin [9] each proved for odd composite n that at least 75% of $a \in \{1, \ldots, n-1\}$ are Miller witnesses for n, which makes Miller's test probabilistic without using GRH.

At the end of [9] Rabin described a second version of Miller's test in terms of confirming or falsifying the congruences in (2.1), attributing this observation to Knuth, and he showed any Miller witness for n is also a Miller–Rabin witness for n in the sense that we defined this term earlier, but Rabin did not indicate if the converse relation is true. Monier [8] confirmed that it is: for each $a \in \{1, \ldots, n-1\}$, the conditions

$$a^{n-1} \not\equiv 1 \bmod n \text{ or } 1 < (a^{2^i k} - 1, n) < n \text{ for some } i \in \{0, \ldots, e-1\} \tag{7.1}$$

and

$$a^k \not\equiv 1 \bmod n \text{ and } a^{2^i k} \not\equiv -1 \bmod n \text{ for all } i \in \{0, \ldots, e-1\} \tag{7.2}$$

are equivalent. Monier used the gcd sequence $(d_0, d_1, \ldots, d_e)$ where $d_i = (a^{2^i k}-1, n)$ to prove the negations of (7.1) and (7.2) are equivalent. Saying (7.1) is false makes the gcd sequence have either the form $(n, \ldots, n)$ with all terms equal to n or the form $(1, \ldots, 1, n, \ldots, n)$ where a sequence of 1's is followed by a sequence of n's (and the last term is n). The first case is equivalent to $d_0 = n$, which says $a^k \equiv 1 \bmod n$, while the second case is equivalent to there being an $i \in \{0, \ldots, e-1\}$ such that $d_i = 1$ and $d_{i+1} = n$, which turns out to be the same as $a^{2^i k} \equiv -1 \bmod n$ (that n is odd is crucial here), and one of those being true is the negation of (7.2).

The Miller–Rabin test had been discovered by Selfridge a couple of years before Miller's paper, but he did not publish anything on it. About 10 years before the work of Miller and Rabin, Artjuhov [1], [2] wrote two papers about primality tests based on congruence conditions. In the Western literature his work is often cited as a version of the Miller–Rabin test that appeared before the work of Miller and Rabin (and Selfridge), but this is incorrect. Artjuhov had instead essentially discovered the Solovay–Strassen test: he proved [1, Theorem E, p. 362] that nonsquare odd composite $n > 1$ have Euler witnesses[6]. While [2] includes the representation of $n-1$ as $2^e k$ and Artjuhov writes in [2] about the congruence $a^k \equiv 1 \bmod n$, he does not consider anything like the additional congruence conditions $a^{2^i k} \equiv -1 \bmod n$.

Appendix A. A probabilistic factorization algorithm

The Miller–Rabin test tells us an odd number is composite with certainty and is prime with a very low probability of error. In the composite case the test does not reveal a factor, so the Miller–Rabin test is not a factorization test. Using ideas behind the Miller–Rabin test with a slight twist, we will be led to a probabilistic algorithm for finding a nontrivial factor of composite odd numbers.

We saw in Corollary 4.2 that when $n > 1$ is odd and not a prime power, the idea behind the Miller–Rabin test works with any $e \geq 1$ and odd positive k, not just those coming from a factorization of $n-1$: over 50% of $a \in \{1, \ldots, n-1\}$ satisfy $a^k \not\equiv 1 \bmod n$ and $a^{2^i k} \not\equiv -1 \bmod n$ for all $i \in \{0, \ldots, e-1\}$. Let's use e and k coming from a factorization of $\varphi(n)$ instead of $n-1$.

[6] Artjuhov's proof is identical to the proof Solovay and Strassen rediscovered in [11]; Solovay and Strassen extended the test to square n in [12].

Theorem A.1. *For odd $n > 1$ that is not a prime power, let $\varphi(n) = 2^e k$ where $e \geq 1$ and k is odd. For at least 50% of $a \in \{1, \ldots, n-1\}$ that are relatively prime to n, the least $j \in \{0, \ldots, e\}$ such that $a^{2^j k} \equiv 1 \bmod n$ is positive and $a^{2^{j-1}k} \not\equiv -1 \bmod n$.*

The table below illustrates the theorem with $n = 15$, so $\varphi(n) = 8 = 2^3 \cdot 1$. Of the eight a relatively prime to 15 in $\{1, \ldots, 14\}$, six fit the conclusion (2, 4, 7, 8, 11, and 13).

a	1	2	4	7	8	11	13	14
j	0	2	1	2	2	1	2	1
$a^{2^{j-1}k} \bmod 15$	X	4	4	4	4	11	4	14

Proof. By Euler's theorem, each $a \in \{1, \ldots, n-1\}$ that is relatively prime to n satisfies $a^{2^e k} \equiv 1 \bmod n$. Thus $a^k \bmod n$ has order dividing 2^e: its order is 2^j for some $j \in \{0, \ldots, e\}$, which means j is minimal such that $a^{2^j k} \equiv 1 \bmod n$. We have $j = 0$ if and only if $a^k \equiv 1 \bmod n$, and for $j \geq 1$ the only $i \in \{0, \ldots, e-1\}$ for which we could have $a^{2^i k} \equiv -1 \bmod n$ is $i = j - 1$.

By the proof of Corollary 4.2, the set of $a \in \{0, \ldots, n-1\}$ such that $a^k \equiv 1 \bmod n$ or $a^{2^i k} \equiv -1 \bmod n$ for some $i \in \{0, \ldots, e-1\}$ is contained in a proper subgroup of the invertible numbers mod n and thus is *at most* half of all a in $\{1, \ldots, n-1\}$ that are relatively prime to n. So for *at least* half of a in $\{1, \ldots, n-1\}$ that are relatively prime to n we have $a^k \not\equiv 1 \bmod n$ and $a^{2^i k} \not\equiv -1 \bmod n$ for all $i \in \{0, \ldots, e-1\}$. Those two conditions are equivalent to saying $j \geq 1$ and $a^{2^{j-1}k} \not\equiv -1 \bmod n$, where j is the order of $a^k \bmod n$. □

When $(a, n) = 1$, rewriting $a^{2^j k} \equiv 1 \bmod n$ from the theorem as $(a^{2^{j-1}k} - 1)(a^{2^{j-1}k} + 1) \equiv 0 \bmod n$ when $j \geq 1$, the first factor can't be a multiple of n by minimality of j, and it can't be relatively prime to n if $a^{2^{j-1}k} \not\equiv -1 \bmod n$. Therefore $1 < (a^{2^{j-1}k} - 1, n) < n$, so $(a^{2^{j-1}k} - 1, n)$ is a nontrivial factor of n and this works at least 50% of the time when $(a, n) = 1$. All a in $\{1, \ldots, n-1\}$ not relatively prime to n give us (a, n) as a nontrivial factor of n, so including these a as well we get (a, n) or $(a^{2^{j-1}k} - 1, n)$ as a nontrivial factor of n over 50% of the time *provided* we know $\varphi(n)$, which is where we get e and k.

Example A.2. Let $n = 12127237$. It turns out that $\varphi(n) = 12119436 = 2^2 \cdot 3029859 = 2^e k$. A random integer from 1 to $n - 1$ is $a = 7169940$. Since $a^k \equiv -1 \bmod n$, this is not helpful. Another random integer is $a = 4689982$, for which $a^k \equiv 2614459 \bmod n$ and $a^{2k} \equiv 1 \bmod n$, so a nontrivial factor of n is $(a^k - 1, n) = (2614458, n) = 5659$: $n = 5659 \cdot 2143$.

The same reasoning would work if $\varphi(n)$ in the theorem were replaced by a multiple of $\varphi(n)$: all we used about e and k was that $a^{2^e k} \equiv 1 \bmod n$ for all a relatively prime to n, and that holds when $2^e k$ is a multiple of $\varphi(n)$. But also it is not realistic (except when thinking about breaking RSA cryptography) to know both n and $\varphi(n)$ without already knowing how to factor n. We modify the factoring procedure as follows to avoid dependence on $\varphi(n)$ in the calculations (only using it in a proof).

Corollary A.3. *For odd $n > 1$ that is not a prime power, over 50% of $a \in \{1, \ldots, n-1\}$ satisfy one the following two conditions.*

(1) $(a, n) > 1$,
(2) $(a, n) = 1$, *$a \bmod n$ has even order t, and $a^{t/2} \not\equiv -1 \bmod n$.*

In the first case, (a, n) is a nontrivial factor of n. In the second case, $(a^{t/2} - 1, n)$ and $(a^{t/2} + 1, n)$ are complementary nontrivial factors of n.

Proof. Let $\varphi(n) = 2^e k$ where $e \geq 1$ and k is odd. By Theorem A.1, for at least 50% of all a in $\{1, \ldots, n-1\}$ that are relatively prime to n the order 2^j of $a^k \bmod n$ has $j \geq 1$ and $a^{2^{j-1}k} \not\equiv -1 \bmod n$. For such a, let $a \bmod n$ have order t. Then $t \mid 2^j k$ since $a^{2^j k} \equiv 1 \bmod n$ and $t \nmid 2^{j-1}k$ since $a^{2^{j-1}k} \not\equiv -1 \bmod n$. Thus the 2-power in t is 2^j, so t is even.

Writing $t = 2^j t'$ for odd t' we have $t' \mid k$. To prove $a^{t/2} \not\equiv -1 \bmod n$ we argue by contradiction. If $a^{t/2} \equiv -1 \bmod n$ then $a^{2^{j-1}t'} \equiv -1 \bmod n$. Raising both sides to the k/t'-power, $a^{2^{j-1}k} \equiv (-1)^{k/t'} \equiv -1 \bmod n$ since k/t' is odd. This contradicts $a^{2^{j-1}k} \not\equiv -1 \bmod n$. We have proved at least 50% of a in $\{1, \ldots, n-1\}$ that are relatively prime to n satisfy condition (2) in the corollary.

From $a^t \equiv 1 \bmod n$ we have $(a^{t/2}+1)(a^{t/2}-1) \equiv 0 \bmod n$. If $(a^{t/2}-1, n) = 1$ then $a^{t/2} + 1 \equiv 0 \bmod n$, but we just saw $a^{t/2} \not\equiv -1 \bmod n$. If $(a^{t/2}-1, n) = n$ then $a^{t/2} \equiv 1 \bmod n$, which contradicts t being the order of $a \bmod n$. Thus $(a^{t/2}-1, n)$ lies strictly between 1 and n when a satisfies (2). It is left to the reader to show $(a^{t/2}+1, n) = n/(a^{t/2}-1, n)$.

Among the a in $\{1, \ldots, n-1\}$, all that are not relatively prime to n satisfy (1) and at least half that are relatively prime to n satisfy (2), so over half satisfy either (1) or (2). □

Corollary A.3 suggests the following algorithm for finding a nontrivial factor of odd composite $n > 1$, preferably to be used only after applying iterations of the Miller–Rabin test to n until we find a witness and thus know n is composite.

Step 1. Check if n is a perfect power: $n \stackrel{?}{=} b^c$ where $b \geq 2$ and $c \geq 2$. (Necessarily $n \geq 2^c$ so $2 \leq c \leq \log_2 n$, and for each such c we can check if $\sqrt[c]{n}$ is an integer or not.) If this happens then b is a nontrivial factor of n and we stop. Otherwise n is not a perfect power and go to the next step.

Step 2. Pick random a in $\{1, \ldots, n-1\}$.

Step 3. Check (by Euclid's algorithm) if $(a, n) > 1$. If so then (a, n) is a nontrivial factor of n and we stop. Otherwise go to the next step.

Step 4. If $(a, n) = 1$ then check if $a \bmod n$ has even order. If the order is odd then return to Step 2.

Step 5. If the order t of $a \bmod n$ is even, check if $a^{t/2} \not\equiv -1 \bmod n$. If so then $(a^{t/2}-1, n)$ is a nontrivial factor of n and stop.

Step 6. If $a^{t/2} \equiv -1 \bmod n$ then return to Step 2.

By Corollary A.3, the probability that a in Step 2 leads to a nontrivial factor of n in Steps 3 or 5 is over 50%, so when n is composite we expect only a few iterations are needed for the algorithm to reveal a nontrivial factor of n. While the Miller–Rabin test itself does not appear in the implementation of Steps 1 through 6, its ideas were used above to justify the 50% lower bound for the algorithm to stop in each round at Steps 3 or 5.

Example A.4. Let $n = 68{,}421{,}093{,}311$. Since $2^{n-1} \equiv 15{,}891{,}188{,}482 \not\equiv 1 \bmod n$, the number n is definitely composite.

A computer's random number generator in the range $[1, n-1]$ spits out first $a = 546{,}802{,}896$. We have $(a, n) = 1$ and the order of $a \bmod n$ is $t = 17{,}091{,}292{,}870$, which is even. Since $a^{t/2} \equiv 31{,}266{,}883{,}924 \not\equiv -1 \bmod n$, a nontrivial factor of n is $(a^{t/2}-1, n) = (31{,}266{,}883{,}923, n) = 2243$. As a check, $n/2243 = 30{,}504{,}277$.

This appears to be a fantastic method of factoring (odd) numbers once we are sure they are composite. But there's a catch, and it's in Step 4: computing the order of $a \bmod n$ in general could take a very long time relative to the size of n on a classical computer. (The numbers in the example are small enough that a classical computer ran each of the steps on them in at most a few seconds.) In the 1990s Peter Shor discovered how to make the calculation of the order of $a \bmod n$ run quickly (polynomial time in $\log n$) on a quantum computer [10]. The six-step algorithm above is called Shor's algorithm.

References

[1] M. M. Artjuhov, "Certain criteria for primality of numbers connected with the little Fermat theorem" (Russian), Acta Arith. **12** (1967), 355–364.

[2] M. M. Artjuhov, "Certain possibilities for a converse to the little Fermat theorem" (Russian), Acta Arith. **13** (1968), 455–464.

[3] E. Bach, "Explicit bounds for primality testing and related problems," Math. Comp. **55** (1990), 355–380.

[4] E. Bach and R. Fernando, "Infinitely many Carmichael Numbers for a Modified Miller–Rabin Test," https://arxiv.org/abs/1512.00444.

[5] M. Dietzfelbinger, *Primality Testing in Polynomial Time: from Randomized Algorithms to "PRIMES is in P"*, Springer-Verlag, Berlin, 2004.

[6] S. B. Gashkov, "Simplified justification of the probabilistic Miller–Rabin test for primality," Discrete Math. Appl. **8** (1998), 545–548. (Translated from Russian, original in Diskret. Mat. **10** (1998), 35–38.)

[7] G. L. Miller, "Riemann's Hypothesis and tests for primality," J. Computer and System Sciences **13** (1976), 300–317.

[8] L. Monier, "Evaluation and comparison of two efficient probabilistic primality testing algorithms," Theoretical Computer Science **12** (1980), 97–108.

[9] M. O. Rabin, "Probabilistic algorithm for testing primality," J. Number Theory **12** (1980), 128–138.

[10] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," https://arxiv.org/pdf/quant-ph/9508027.pdf.

[11] R. M. Solovay and V. Strassen, "A fast Monte-Carlo test for primality," SIAM Journal on Computing **6** (1977), 84-85.

[12] R. M. Solovay and V. Strassen, "Erratum: A fast Monte-Carlo test for primality," SIAM Journal on Computing **7** (1978), 1.