# 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 $n$, and the proportion exceeds 75% except when $n = 9$. This is much 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 $n$, 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 mod $n$, 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 $a \in \{1,\dots,n-1\}$. We say $a$ is a Miller–Rabin witness for $n$ if all of the congruences in* (2.1) *are false:*

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

*We say $a$ is a Miller–Rabin nonwitness for $n$ if one of the congruences in* (2.1) *is true:*

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

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 $i \in \{1,\dots,e-1\}$, 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 if $a^{(n-1)/2} \equiv \pm 1 \bmod n$.

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

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

with all terms considered mod $n$. We call this the *Miller–Rabin sequence* for $n$ that is generated by $a$. For example, to compute the Miller–Rabin sequence for 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

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

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 $n = 29341$. 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 2.6.** 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 2.7.** 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 smallest odd composite number that does not have either 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 composite integer 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.

Here is yet another way to think about Miller–Rabin witnesses. When $n$ is 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 $2^j$ where $j \in \{1, \ldots, e\}$, 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 a number modulo $n$ that would have to be a square root of unity besides $\pm 1 \bmod n$, which would be impossible if $n$ were prime.

It turns out that Euler witnesses are always Miller–Rabin witnesses (Theorem 5.1), and sometimes they are the same set of numbers (Corollary 5.2), but when there are more Miller–Rabin witnesses than Euler witnesses there can be a lot more. Sometimes the change is not very impressive, such as for 30121, whose proportion of Euler witnesses is already quite high at 96.4% and its proportion of Miller–Rabin witnesses is 99.1%. But for 75361 the proportion of Euler witnesses is 61.7% while the proportion of Miller–Rabin witnesses is 99.4%.

The next theorem quantifies how large the proportion of Miller–Rabin witnesses must be for an odd composite number.

**Theorem 2.8.** *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%.*

This will be proved in Section 4. The 75% lower bound is probably sharp: if $p$ and $2p-1$ are both odd primes then the proportion of Miller–Rabin witnesses for $n = p(2p-1)$ tends to 75% if we can let $p \to \infty$. (It is believed that $p$ and $2p - 1$ are both prime infinitely often.)

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 2.8.

(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 2.8 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 6.

## 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

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

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 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 proportion of Fermat nonwitnesses (for non-Carmichael $n$) and Euler nonwitnesses is less than 50% when $n$ is composite, which makes the proportion of witnesses 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.

[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.

**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 $n$ that guarantee the Miller–Rabin nonwitnesses are a group under multiplication mod $n$.

**Theorem 3.3.** *If $n > 1$ is odd and $-1 \not\equiv \square \bmod n$ then the set of 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 $-1 \not\equiv \square \bmod n$ 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 $n$. □

A simple situation where $-1 \not\equiv \square \bmod n$ is if $n \equiv 3 \bmod 4$, and in this case the description of the Miller–Rabin nonwitnesses as $\{1 \leq a \leq n-1 : a^{(n-1)/2} \equiv \pm 1 \bmod n\}$ can also be seen directly from the definition of a nonwitness using $e = 1$.

Another example where the Miller–Rabin nonwitnesses form a group is $n = p^\alpha$ for an odd prime $p$ and $\alpha \geq 1$. (We allow $\alpha = 1$, corresponding to $n = p$ being prime, since what we say will be valid in that case.)

**Theorem 3.4.** *For a prime power $p^\alpha$ where $\alpha \geq 1$, the Miller–Rabin nonwitnesses for $p^\alpha$ are the solutions in $\{1, \ldots, p^\alpha - 1\}$ to $a^{p-1} \equiv 1 \bmod p^\alpha$, which form a group under multiplication mod $n$.*

*Proof.* Let $a \in \{1, \ldots, p^\alpha - 1\}$ be a Miller–Rabin nonwitness. Since $a$ is relatively prime to $p^\alpha$, Euler's theorem tells us $a^{\varphi(p^\alpha)} \equiv 1 \bmod p^\alpha$, so $a^{p^{\alpha-1}(p-1)} \equiv 1 \bmod p^\alpha$. At the same time, as a nonwitness we have either $a^k \equiv 1 \bmod p^\alpha$ or $a^{2^i k} \equiv -1 \bmod p^\alpha$ for some $i \leq e-1$, and both cases imply $a^{2^e k} \equiv 1 \bmod p^\alpha$, or equivalently $a^{p^\alpha - 1} \equiv 1 \bmod p^\alpha$. Thus the order of $a \bmod p^\alpha$ divides $(p^{\alpha-1}(p-1), p^\alpha - 1)$. 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 $f \geq 1$ and $\ell$ is odd. Since $p-1$ is a factor of $p^\alpha - 1 = 2^e k$, we have $f \leq e$ and $\ell \mid k$. Since $(a^\ell)^{2^f} \equiv 1 \bmod p^\alpha$, the order of $a^\ell \bmod p^\alpha$ is $2^i$ for some $j \in \{0, \dots, f\}$.

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 $j \geq 1$, 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 $p^\ell$. 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 $k/\ell$ power gives us $a^{2^i k} \equiv -1 \bmod p^\alpha$ where $i = j - 1 \in \{0, \dots, f-1\} \subset \{0, \dots, e-1\}$. $\square$

The sufficient conditions in Theorems 3.3 and 3.4 turn out to be necessary too: for odd $n > 1$ such that $-1 \equiv \square \bmod n$ 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 Section 4. This allows work on the Generalized Riemann Hypothesis (GRH) as described at the end of Section 3 to be applied to the Miller–Rabin test: if GRH is true then any odd composite $n > 1$ has a Miller–Rabin witness $\leq 2(\log n)^2$, so GRH implies the Miller–Rabin test can be made deterministic in polynomial time.

## 4. A proof of the bound on Miller–Rabin witnesses

In this section we will prove Theorem 2.8. Rather than prove the proportion of Miller–Rabin witnesses 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 $p^\alpha$ are the solutions to $a^{p-1} \equiv 1 \bmod p^\alpha$. Such $a$ are closed under multiplication, 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 $\alpha$ small. We include $\alpha = 1$.

| $\alpha$ | 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 |

[2] What we just proved, that the only solutions to $x^2 = 1$ modulo an odd prime power are $\pm 1$, will be used again in our proof of Theorem 2.8. It is *false* for powers of 2 starting with 8: modulo $2^\alpha$ for any $\alpha \geq 3$ there are 4 square roots of unity.

This suggests $a^{p-1} \equiv 1 \bmod p^\alpha$ has $p-1$ solutions mod $p^\alpha$ for each $\alpha$, which is clear when $\alpha = 1$ by Fermat's little theorem. For larger $\alpha$ 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 $p^\alpha$, their density is

$$\frac{p-1}{p^\alpha - 1} = \frac{1}{1+p+\cdots+p^{\alpha-1}}. \tag{4.1}$$

Since $\alpha \geq 2$ ($p^\alpha$ is not prime!) this ratio is at most $1/(1+p)$, which in turn is at most $1/(1+3) = 1/4$, and the only way (4.1) equals $1/4$ is if $\alpha = 2$ and $p = 3$, *i.e.*, $n = 3^2 = 9$. For any other $p^\alpha$ the value of (4.1) is less than $1/4$, while for $p^\alpha = 9$ the density is $1/4$.

From now on let $n$ have at least two prime factors. Write, as usual, $n - 1 = 2^e k$ with $e \geq 1$ and $k$ odd. Let $n$ have the distinct prime factors $p_1, \ldots, p_r$ (so $r \geq 2$) and let $2^{v_j}$ be the highest power of 2 that divides $p_j - 1$, so $v_j \geq 1$. Set

$$v = \min(v_1, \ldots, v_r) \geq 1. \tag{4.2}$$

**Lemma 4.1.** *With notation as above, we have*

1) $v \leq e$,
2) *if the congruence* $x^{2^i k} \equiv -1 \bmod n$ *has a solution then* $i < v$,
3) *if* $a \in \{1, \ldots, n-1\}$ *is not a Miller–Rabin witness for* $n$ *then* $a^{2^v k} \equiv 1 \bmod n$.

*Proof.* 1) Since $2^{v_j} \mid (p_j - 1)$ we have $2^v \mid (p_j - 1)$ for all $j$, so $p_j \equiv 1 \bmod 2^v$. Thus $n \equiv 1 \bmod 2^v$, so $2^v \mid (n-1)$, which makes $v \leq e$.

2) Suppose $x \in \mathbf{Z}$ satisfies $x^{2^i k} \equiv -1 \bmod n$ with $i \geq v$. We will get a contradiction.

Without loss of generality, let $v = v_1$ and set $p_1 - 1 = 2^{v_1}k_1$. From $i \geq v_1$ reducing the congruence $a^{2^i k} \equiv -1 \bmod n$ to $a^{2^i k} \equiv -1 \bmod p_1$ and raising both sides to the $k_1$-th power (an odd power) gives us $a^{2^i k k_1} \equiv -1 \bmod p_1$. But $2^i k_1$ is a multiple of $p_1 - 1$ since $i \geq v_1$, so $a^{2^i k k_1} \equiv 1 \bmod p$ by Fermat's little theorem. This is a contradiction, so $i < v_1$.

3) We want to show that if $a^k \equiv 1 \bmod n$ or $a^{2^i k} \equiv -1 \bmod n$ for some $i \in \{0, \ldots, e-1\}$ then $a^{2^v k} \not\equiv 1 \bmod n$. Certainly from $a^k \equiv 1 \bmod n$ we get $a^{2^v k} \equiv 1 \bmod n$. If there's an $i \in \{0, \ldots, e-1\}$ such that $a^{2^i k} \equiv -1 \bmod n$ then $i < v$ by part 2, so by squaring that congruence enough times we get $a^{2^v k} \equiv 1 \bmod n$. □

**Lemma 4.2.** *If* $a \in \{1, \ldots, n-1\}$ *is not a Miller–Rabin witness for* $n$ *then* $a^{2^{v-1}k} \equiv \pm 1 \bmod n$, *where* $v$ *is defined in* (4.2).

*Proof.* By part 3 of Lemma 4.1, $a^{2^v k} \equiv 1 \bmod n$. That $a$ is not a Miller–Rabin witness for $n$ means either $a^k \equiv 1 \bmod n$ or $a^{2^i k} \equiv -1 \bmod n$ for some $i \in \{0, \dots, e-1\}$. We will show either condition implies $a^{2^{v-1}k} \equiv \pm 1 \bmod n$.

If $a^k \equiv 1 \bmod n$ then obviously $a^{2^{v-1}k} \equiv 1 \bmod n$. If $a^{2^i k} \equiv -1 \bmod n$ then $i < v$ by part 2 of Lemma 4.1. If $i = v-1$ then of course $a^{2^{v-1}k} \equiv -1 \bmod n$. If $i < v-1$ then $a^{2^i k} \equiv -1 \bmod n \Rightarrow a^{2^{v-1}k} \equiv 1 \bmod n$ by squaring enough times. □

Lemma 4.2 gives us a fundamental containment: for odd composite $n > 1$ that is not a prime power,

$$\{\text{Miller–Rabin nonwitnesses for } n\} \subset \{1 \le a \le n-1 : a^{2^{v-1}k} \equiv \pm 1 \bmod n\}. \tag{4.3}$$

What makes this important is that although the left side may not be a group under multiplication mod $n$ the right side is![3] Set

$$G_n = \{1 \le a \le n-1 : a^{2^{v-1}k} \equiv 1 \bmod n\},$$

which is a subgroup of the invertible numbers mod $n$. If the congruence $x^{2^{v-1}k} \equiv -1 \bmod n$ has no solution then the right side of (4.3) is $G_n$. If there is a solution, say $x = b$, then the right side of (4.3) is $G_n \cup bG_n$ (as a set of integers modulo $n$). Either way, the size of the right side of (4.3) is at most $2|G_n|$, so

$$\text{proportion of Miller–Rabin nonwitnesses for } n = \frac{|\{\text{MR nonwitnesses for } n\}|}{n-1} \le \frac{2|G_n|}{n-1}.$$

We will show $2|G_n|/(n-1) < 1/4$ if $n \neq 9$.

Set

$$\widetilde{G}_n = \{1 \le a \le n-1 : a^{2^v k} \equiv 1 \bmod n\}. \tag{4.4}$$

This is a subgroup of the invertible numbers mod $n$ and $G_n$ is a subgroup of it. Since $n$ is not prime we have $\varphi(n) < n-1$, so

$$\frac{2|G_n|}{n-1} = \frac{2|G_n|}{|\widetilde{G}_n|} \cdot \frac{|\widetilde{G}_n|}{n-1} < \frac{2|G_n|}{|\widetilde{G}_n|} \cdot \frac{|\widetilde{G}_n|}{\varphi(n)}.$$

Since a strict inequality appears here, to show $2|G_n|/(n-1) < 1/4$ it would suffice to have

$$\frac{2|G_n|}{|\widetilde{G}_n|} \cdot \frac{|\widetilde{G}_n|}{\varphi(n)} \le \frac{1}{4},$$

which is equivalent to

$$\frac{|\widetilde{G}_n|}{|G_n|} \cdot \frac{\varphi(n)}{|\widetilde{G}_n|} \ge 8. \tag{4.5}$$

Since $G_n$ is a subgroup of $\widetilde{G}_n$ and $\widetilde{G}_n$ is a subgroup of the invertible numbers modulo $n$, the ratios $|\widetilde{G}_n|/|G_n|$ and $\varphi(n)/|\widetilde{G}_n|$ are integers. Is their product at least 8?

**Lemma 4.3.** *The ratio $|\widetilde{G}_n|/|G_n|$ is $2^r$, where $r$ is the number of distinct prime factors of $n$.*

[3] In fact, Jim Haglund showed the set on the right side of (4.3) is the subgroup mod $n$ generated by the Miller–Rabin nonwitnesses for $n$. We will not need this, but it shows (4.3) is the optimal containment we can hope for that has a group on the right side.

*Proof.* We will make a homomorphism from $\widetilde{G}_n$ onto a group of order $2^r$ with kernel $G_n$.

The distinct prime factors of $n$ are $p_1, \dots, p_r$. Let the prime power factorization of $n$ be $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Then

$$x \equiv y \bmod n \Longleftrightarrow x \equiv y \bmod p_j^{\alpha_j} \text{ for } j = 1, \dots, r.$$

For $a \in \widetilde{G}_n$ we have $a^{2^v k} \equiv 1 \bmod n$, which is equivalent to $(a^{2^{v-1}k})^2 \equiv 1 \bmod p_j^{\alpha_j}$ for all $j$. Modulo any odd prime power the only square roots of 1 are $\pm 1$, as we saw in the proof of Theorem 3.4, so

$$a^{2^v k} \equiv 1 \bmod p_j^{\alpha_j} \Longleftrightarrow a^{2^{v-1}k} \equiv \pm 1 \bmod p_j^{\alpha_j}.$$

Thus

$$a \bmod n \in \widetilde{G}_n \Longleftrightarrow a^{2^{v-1}k} \equiv \pm 1 \bmod p_j^{\alpha_j} \text{ for } j = 1, \dots, r.$$

In this equivalence, elements on the left in $G_n$ correspond to the congruence conditions $a^{2^{v-1}k} \equiv 1 \bmod p_j^{\alpha_j}$ for all $j$ on the right. So the mapping $f \colon \widetilde{G}_n \to \prod_{j=1}^r \{\pm 1 \bmod p_j^{\alpha_j}\}$ defined by

$$f(a \bmod n) = (\dots, a^{2^{v-1}k} \bmod p_j^{\alpha_j}, \dots)_{j=1}^r$$

is a homomorphism of groups with kernel $G_n$. The target group has order $2^r$, so our remaining task is to prove $f$ is surjective.

It suffices, since $f$ is multiplicative, to show the $r$-tuples $(\dots, 1, -1, 1, \dots)$ with a single $-1$ in one component and 1 in the other components is in the image of $f$. By symmetry it's enough to show $(-1, 1, 1, \dots, 1)$ is in the image of $f$. That is, we seek an $a \in \widetilde{G}_n$ such that

$$a^{2^{v-1}k} \equiv \begin{cases} -1 \bmod p_1^{\alpha_1}, \\ \ \ 1 \bmod p_j^{\alpha_j}, \text{ if } j > 1. \end{cases}$$

Since $k$ is odd, what we're going to do is find a $b$ such that

$$b^{2^{v-1}} \equiv \begin{cases} -1 \bmod p_1^{\alpha_1}, \\ \ \ 1 \bmod p_j^{\alpha_j}, \text{ if } j > 1 \end{cases}$$

and then $a := b^k \bmod n$ does what we want.

Recall $v = \min v_j$, so $v \le v_1$. Since $2^{v_1}$ is the highest power of 2 dividing $p_1 - 1$, also $2^v \mid (p_1 - 1)$. We want to show some number mod $p_1^{\alpha_1}$ has order $2^v$ and will then get $b$ from that with the Chinese remainder theorem.

We saw in Section 3 that for any odd prime power $p^\alpha$ there are $p - 1$ solutions to $x^{p-1} \equiv 1 \bmod p^\alpha$, each one reducing to a different value mod $p$. The nonzero numbers mod $p$ contain a generator, say $g$, meaning $g \bmod p$ has order $p - 1$. Letting $g_\alpha \bmod p^\alpha$ be the solution of $x^{p-1} \equiv 1 \bmod p^\alpha$ such that $g_\alpha \equiv g \bmod p$, the order of $g_\alpha \bmod p^\alpha$ is also $p - 1$: if $m$ is the order of $g_\alpha \bmod p^\alpha$ then $g_\alpha^m \equiv 1 \bmod p^\alpha$ so $m \mid (p-1)$. Reducing the congruence to modulus $p$ makes $g^m \equiv 1 \bmod p$, so $(p - 1) \mid m$, and thus $m = p - 1$.

Taking $p = p_1$, there is an integer mod $p_1^{\alpha_1}$ with order $p_1 - 1$. A suitable power of it can have order equal to any factor of $p_1 - 1$ that we want, so some number mod $p_1^{\alpha_1}$ has order $2^v$. Call that element $c$, so $c^{2^{v-1}} \not\equiv 1 \bmod p_1^{\alpha_1}$ but $(c^{2^{v-1}})^2 \equiv 1 \bmod p_1^{\alpha_1}$. This forces $c^{2^{v-1}} \equiv -1 \bmod p_1^{\alpha_1}$. Now we can define $b$: let it be a solution to the system of congruences

$$b \equiv c \bmod p_1^{\alpha_1} \text{ and } b \equiv 1 \bmod p_j^{\alpha_j} \text{ for } j > 1.$$

By the Chinese remainder theorem there is a unique such $b$ modulo $p_1^{\alpha_1} \cdots p_r^{\alpha_r} = n$. □

By Lemma 4.3, if $r \geq 3$ then $|\widetilde{G}_n|/|G_n| \geq 8$, so (4.5) holds, as $\varphi(n)/|\widetilde{G}_n| \geq 1$. If $r = 2$ then the left side of (4.5) is

$$\frac{|\widetilde{G}_n|}{|G_n|} \cdot \frac{\varphi(n)}{|\widetilde{G}_n|} = 4\frac{\varphi(n)}{|\widetilde{G}_n|},$$

and this is at least 8 if and only if $\varphi(n)/|\widetilde{G}_n| \geq 2$, which is equivalent to $\varphi(n)/|\widetilde{G}_n| > 1$ since $\varphi(n)/|\widetilde{G}_n|$ is an integer. Why is $|\widetilde{G}_n| < \varphi(n)$? Since $2^v k$ is a factor of $2^e k = n-1$ (recall $v \leq e$ by part 1 of Lemma 4.1), every $a \in \widetilde{G}_n$ satisfies $a^{n-1} \equiv 1 \bmod n$. Because $n$ has two prime factors while Carmichael numbers have at least three prime factors, $n$ is not a Carmichael number and thus some integer relatively prime to $n$ doesn't satisfy $a^{n-1} \equiv 1 \bmod n$, so $a \notin \widetilde{G}_n$ and thus $|\widetilde{G}_n| < \varphi(n)$.

Our proof of Theorem 2.8 is now complete.

**Corollary 4.4.** *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 (4.3) shows us the Miller–Rabin nonwitnesses for $n$ lie in a group of order at most $2|G_n|$, and we will show $2|G_n| < \varphi(n)$, or equivalently $\varphi(n)/|G_n| > 2$. From the proof of Theorem 2.8,

$$\frac{\varphi(n)}{|G_n|} = \frac{|\widetilde{G}_n|}{|G_n|}\frac{\varphi(n)}{|\widetilde{G}_n|} = 2^r\frac{\varphi(n)}{|\widetilde{G}_n|}.$$

Since $2^r \geq 4$ and $\varphi(n)/|\widetilde{G}_n| \geq 1$, we're done. □

Gashkov [4] gave another proof of this theorem. 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.

## 5. 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 2.8 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 5.1.** *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 $2^ik$ for $0 \leq i \leq e-1$, 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.

Case 1: $e = 1$, 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 $2^ik$ for every $i \in \{0, \ldots, e-2\}$.

If $a^k \equiv 1 \bmod n$ or $a^{2^ik} \equiv -1 \bmod n$ 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

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

and

$$a^{(n-1)/2} \equiv -1 \bmod n \Longrightarrow \left(\frac{a}{n}\right) = -1. \tag{5.1}$$

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 $a^{2^ik} \equiv -1 \bmod n$ 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 $a^{2^ik} \equiv -1 \bmod n$ that

$$\left(\frac{a}{n}\right) = \begin{cases} -1 \bmod n, & \text{if } i = e-1, \\ \ \ 1 \bmod n, & \text{if } 0 \leq i \leq e-2 \end{cases} \tag{5.2}$$

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 $p \mid n$ write $p - 1 = 2^{v_p}k_p$ where $v_p \geq 1$ and $k_p$ is odd. From the proof of part 2 of Lemma 4.1, the condition $a^{2^ik} \equiv -1 \bmod n$ implies $i < v_p$ (let $v_1$ in Lemma 4.1 be replaced by $v_p$ here). Thus every $p-1$ is divisible by $2^{i+1}$. In terms of congruences,

$$p \equiv 1 \bmod 2^{i+1} \tag{5.3}$$

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

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 $(\frac{a}{p}) \equiv a^{(2^ik)(2^{v_p-1-i}k_p)} \equiv (-1)^{2^{v_p-1-i}} \bmod p$. 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

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & \text{if } i = v_p - 1 \ \ (\text{equiv., } v_p = i+1), \\ \ \ 1, & \text{if } i < v_p - 1 \ \ (\text{equiv., } v_p > i+1). \end{cases} \tag{5.4}$$

The congruence (5.3) 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 (5.4) 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

$$n \equiv 1 + c2^{i+1} \bmod 2^{i+2}. \tag{5.5}$$

Recall $n - 1 = 2^e k$ with $k$ odd, so (5.5) says $1 + 2^e k \equiv 1 + c2^{i+1} \bmod 2^{i+2}$. Also recall $0 \leq i \leq e-1$. 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 $i+2 \leq e$, 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 (5.2). □

**Corollary 5.2.** *If $n \equiv 3 \bmod 4$, Euler witnesses and Miller–Rabin witnesses for $n$ coincide.*

*Proof.* In Case 1 of the proof of Theorem 5.1 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 5.2 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 5.3.** *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 $i = e - 1 \geq 1$) 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 (5.1). □

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 $n \equiv 1 \bmod 4$.

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

## 6. The original version of the Miller–Rabin test

The Miller–Rabin test was introduced by Miller [5], 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 Rabin [7] 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 [7] 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 [6] confirmed that it is: for each $a \in \{1, \ldots, n-1\}$, the conditions

$$a^{n-1} \not\equiv 1 \bmod n \text{ or } 1 < (a^{2^i k} - 1, n) < n \text{ for some } i \in \{0, \ldots, e-1\} \tag{6.1}$$

and

$$a^k \not\equiv 1 \bmod n \text{ and } a^{2^i k} \not\equiv -1 \bmod n \text{ for all } i \in \{0, \ldots, e-1\} \tag{6.2}$$

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 (6.1) and (6.2) are equivalent. Saying (6.1) 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 (6.2).

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, but this is incorrect. The paper [1] is about the Solovay–Strassen test; Artjuhov essentially proved odd composite $n > 1$ have Euler witnesses. While his paper [2] does include the representation of $n-1$ as $2^e k$ and he writes about the congruence $a^k \equiv 1 \bmod n$, he does not consider anything like the additional congruence conditions $a^{2^i k} \equiv -1 \bmod n$.

## References

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

[2] M. M. Artjuhov, "On 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] 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.)

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

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

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