23 Primality Testing

One of the most important problems in the field of computer science is a math problem as well: *How can we determine if an integer n is prime?*

This chapter is devoted to primality testing. Primality testing has applications in many fields, including cryptography (see, for example, the RSA [61] algorithm), hash function design, pseudo-random number generation, and many others.

23.1 Naive Algorithms

Question: Think for a minute on how you might try to determine if n is prime or composite.

Answer: Back in grade school, you might have approached this question by considering every integer $k \in S = \{2, 3, 4, \ldots, n-1\}$ and asking whether k divides n, written $k \mid n$.

Definition 23.1 *If we find some $k \in S = \{2, 3, 4, \ldots, n-1\}$ such that $k \mid n$, then we say that k is a* **witness** *to the fact that n is composite. To be specific, we will say that k is a* **divisor witness** *to n being composite.*

You might improve upon this method by only considering divisors up to $\lfloor \sqrt{n} \rfloor$, that is, $S = \{2, 3, 4, \ldots, \lfloor \sqrt{n} \rfloor\}$. You can improve further by eliminating all multiples of 2 in S, other than 2, and then removing all multiples of 3 in S, other than 3, and so on. This process of removing all multiples of every prime in sequence is known as the Sieve of Eratosthenes.

Question: Suppose we've winnowed down the set S of potential divisors of n to just those primes which are smaller than n. It seems our test set should now be small. How big is our test set?

Answer: It turns out that the number of primes less than n is $\Theta\left(\frac{n}{\ln n}\right)$. This result

is known as the Prime Number Theorem (see [24, 68]). Thus, even the winnowed down set S still has size which grows quickly with n.

Our goal in this chapter is to find a constant-time Monte Carlo style test to determine, with high probability, whether n is prime.

Importantly, this high probability of correctness should apply equally well to every n.

Question: For example, what's wrong with an algorithm that checks only if n is divisible by 2, 3, and 5, returning "probably prime" if none of those are divisors?

Answer: There is a significant fraction of composite numbers whose compositeness would never be detected by the above test. We want *every* n to have a high probability of correctly being evaluated, where the probability of error is exponentially decreasing in the number of random trials.

In Sections 23.2 and 23.3 we introduce the Fermat Primality Test. This test has the advantage of being very simple. Unfortunately, there is a *tiny* fraction of composite numbers, known as Carmichael numbers, for which the Fermat test will almost always return "prime." Thus the Fermat Primality Test is not a true test for primality.

In Section 23.4 we introduce a more complex test, called the Miller–Rabin test. The Miller–Rabin test works for all numbers, including Carmichael numbers. The Miller–Rabin test builds upon the Fermat test, so it's worth going through the sections in order. The Miller–Rabin test is the most practical and most widely used primality testing algorithm. It appears in software libraries for encryption schemes, such as RSA.

23.2 Fermat's Little Theorem

We normally think of a prime number as a whole number, greater than 1, whose only positive divisors are 1 and itself. The Fermat test is based on Fermat's Little Theorem, which provides an alternative characterization of prime numbers.

Theorem 23.2 (Fermat's Little Theorem) *The number n is prime if and only if*

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

for every *integer* $a \in S = \{1, 2, 3, \ldots, n-1\}$.

We will prove Theorem 23.2 later in this section. For now, observe that Theorem 23.2 says two things:

- If n is **prime**, then $a^{n-1} \equiv 1 \bmod n$, for every $a \in S$.
- If n is **composite**, then $a^{n-1} \not\equiv 1 \bmod n$, for at least one $a \in S$.

Definition 23.3 *Suppose n is composite. Consider*

$$T = \{a : a < n \text{ and } a^{n-1} \not\equiv 1 \bmod n\}.$$

The elements of T are called **Fermat witnesses** *to the fact that n is composite.*

Question: We have talked about two different types of witnesses to n being composite: divisor witnesses and Fermat witnesses. For a given composite n, are there more Fermat witnesses, or divisor witnesses?

Answer: It turns out that there are typically way more Fermat witnesses than divisor witnesses, which makes it much easier to find a Fermat witness. In fact, every divisor witness is also a Fermat witness.

For example, consider $n = 15$. The divisor witnesses of n's compositeness are 3 and 5. However, the set of Fermat witnesses is $\{2, 3, 5, 6, 7, 8, 9, 10, 12, 13\}$.

Theorem 23.4 *For every composite number n, every divisor witness of n is also a Fermat witness.*

Proof: Let $d > 1$ be a divisor of n. We'll show that d is a Fermat witness for n.

Suppose by contradiction that

$$d^{n-1} \equiv 1 \bmod n.$$

This means that there's some integer q such that

$$d^{n-1} = qn + 1. \tag{23.1}$$

But (23.1) can't be true because d divides the first term and the second term (since d divides n), but not the third term. Hence we have a contradiction. ■

Before we can prove Fermat's Little Theorem (Theorem 23.2), we need one quick fun fact about prime numbers.

Lemma 23.5 (Fun fact about primes) *If $p > 2$ is prime, then $\forall$ integers a, b,*

$$(a+b)^p \equiv a^p + b^p \bmod p$$
$$(a-b)^p \equiv a^p - b^p \bmod p.$$

Proof: If we write out the binomial expansion of $(a+b)^p$, it will be the case that every term in the expansion, other than the first or last term, is divisible by p. To see this, consider an arbitrary term in the expansion, say one with coefficient

$$\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k(k-1)(k-2)\cdots 1}.$$

Observe that there is a factor p in the numerator, which is prime and thus not canceled by any terms in the denominator. Hence this term equals 0 mod p. The case of $(a-b)^p$ is similar, but requires that p is odd. ■

We are now ready to prove Fermat's Little Theorem (Theorem 23.2).

Proof: [Theorem 23.2] Suppose n is composite. We need to show that there's at least one integer $a < n$ such that $a^{n-1} \not\equiv 1 \bmod n$. This is easy: We know that n has some divisor, d. But then, by Theorem 23.4, we know that d is also a Fermat witness. Thus $d^{n-1} \not\equiv 1 \bmod n$.

Suppose now that n is prime. If $n = 2$, Fermat's Little Theorem holds trivially. So assume $n > 2$. Let's define set W to be the following set of integers:

$$W = \{x : x^n \equiv x \bmod n\}.$$

Question: Is the integer 1 contained in W?

Answer: Yes.

Question: Once we know that 1 is in W, what does the Fun Fact tell us about 2?

Answer: 2 is also in W.

In fact, the Fun Fact tells us that the set W is closed under addition and subtraction. To see this, observe that if $a, b \in W$, then $(a+b)^p \equiv a^p + b^p \equiv a + b \bmod p$, so $a + b \in W$ as well. The argument is similar for $a - b$.

So W contains all integers!

Now consider any integer $x \in S = \{1, 2, 3, \ldots n-1\}$, where n is a prime. We will use the fact that any such $x \in S$ is also in W to show that x has the property that $x^{n-1} \equiv 1 \bmod n$.

First observe that since $x \in W$, we know that n divides $x^n - x$, so

$$n \Big| x\left(x^{n-1} - 1\right). \tag{23.2}$$

But since $x < n$, we also know that x is not divisible by n. So, since n is prime, and it doesn't divide the first term in (23.2), it must divide the second term, $x^{n-1} - 1$. Thus,

$$x^{n-1} - 1 \equiv 0 \bmod n$$

and we're done. ■

Let's define one more type of witness for compositeness:

Definition 23.6 *Given a composite number n, let $a \in \{1, 2, \ldots n-1\}$ have the property that $\gcd(a, n) > 1$. Then we say that a is a* **gcd witness** *of n's compositeness.*

Theorem 23.4 can be made more general, as shown in Theorem 23.7.

Theorem 23.7 *For every composite number n, every divisor witness of n's compositeness is also a gcd witness, and every gcd witness is also a Fermat witness.*

Proof: See Exercise 23.1. ■

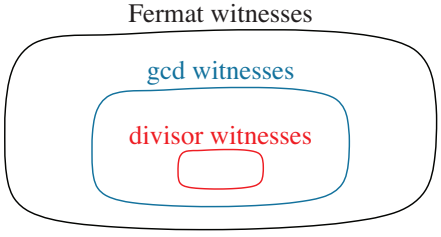

Figure 23.1 *Illustration of Theorem 23.7.*

Again, what's important is that while the number of divisor witnesses and gcd witnesses is very small, the number of Fermat witnesses is typically very high, making them easy to find. As another typical example, consider $n = 415{,}693$. There are only two divisor witnesses of n, namely 593 and 701. While there are more gcd witnesses, the proportion of gcd witnesses is still less than 1% (most numbers are relatively prime to n). By contrast, the proportion of Fermat witnesses is over 99%.

23.3 Fermat Primality Test

The Fermat Primality Test is motivated by the fact that there are typically so many Fermat witnesses. Given an integer n, the test considers a random number less than n and checks whether that number is a Fermat witness.

Algorithm 23.8 (Fermat Primality Test)
We are given an integer n which we wish to classify as prime or composite. Repeat the following for k rounds:

1. *Choose $a \in S = \{1, 2, 3, \ldots, n-1\}$ uniformly at random.*
2. *If $a^{n-1} \not\equiv 1 \bmod n$, return COMPOSITE and stop.*

If we haven't stopped after k rounds, then return PROBABLY PRIME.

The Fermat Primality Test has **one-sided error**. If the test returns "composite" then n is provably composite (since a Fermat witness of compositeness was found). On the other hand, if the test returns "probably prime" then n might be prime, or we might simply have gotten unlucky and not found a Fermat witness.

So *mistakes* happen when n is composite but a Fermat witness is not found. What is the probability of a *mistake*?

We know, by Theorem 23.4, that every composite number, n, has at least two Fermat witness (the divisors of n are Fermat witnesses). To understand the probability of a mistake, we need to understand:

Given that n is composite, how many Fermat witnesses does n have?

Question: Suppose that we could say that for every composite number n, at least half the $a \in S = \{1, 2, 3, \ldots, n-1\}$ are Fermat witnesses. What would be the accuracy of the Fermat Primality Test?

Answer: In the case where n is composite, the Fermat Primality Test would return "composite" with probability at least $1 - 2^{-k}$. Note that there's never any error in the case where n is prime.

Unfortunately, while the proportion of Fermat witnesses is typically very high, it is not always true that at least half the $a \in S$ are Fermat witnesses. Here is what we do know: Consider the set $\mathcal{F}$ of Fermat witnesses of some composite number n, as shown in Figure 23.2. By Theorem 23.7, all gcd witnesses of n are automatically included in $\mathcal{F}$; we refer to these gcd witnesses as **trivial Fermat witnesses**. Unfortunately, there are typically very few gcd witnesses, and thus very few trivial Fermat witnesses. Suppose now that there is a **non-trivial Fermat**

witness for n, that is, some $a \in \{1, 2, \ldots, n-1\}$ where a is relatively prime to n and is a Fermat witness. Theorem 23.9 tells us that as soon as there is a single *non-trivial* Fermat witness, then we know that the total proportion of Fermat witness is at least half.

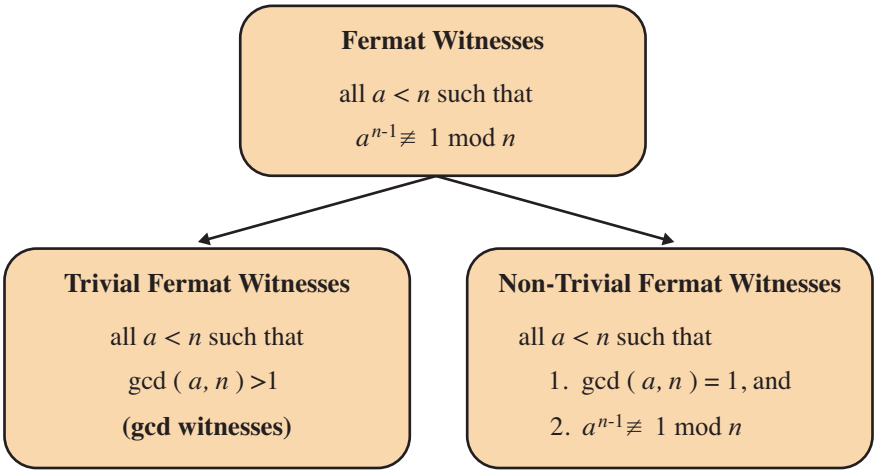

Figure 23.2 *Two types of Fermat witnesses for composite number n.*

Theorem 23.9 *For composite number n, suppose that there is at least one a in* $S = \{1, 2, 3, \ldots, n-1\}$ *such that a is a Fermat witness for n and* $\gcd(a, n) = 1$. *Then at least half the elements of S are Fermat witnesses for n.*

Proof: We defer the proof to Section 23.6. ■

So it seems that if there's even just *one* non-trivial Fermat witness for n, then it follows that there are plenty of Fermat witnesses for n. Unfortunately, there exists a very small set of composite numbers for which there are *zero* non-trivial Fermat witnesses. These numbers are called Carmichael numbers.

Definition 23.10 *A* **Carmichael number** *is a composite integer n such that,* $\forall a \in S = \{1, 2, 3, \ldots, n-1\}$*:*

$$\text{if } \gcd(a, n) = 1, \quad \text{then} \quad a^{n-1} \equiv 1 \bmod n.$$

Because this holds for all a, the Carmichael numbers have zero non-trivial Fermat witnesses.

The Carmichael numbers are named after Robert Carmichael [12, 13]. The first few numbers are:

$$561 \qquad 1105 \qquad 1729$$

Carmichael numbers are still a topic of current study by number theorists. The Carmichael numbers have several interesting properties (see [30]). They are odd, each having at least three distinct prime factors. They are square free (not divisible by the square of any prime), and for every Carmichael number n with prime factor p, it holds that $p - 1$ divides $n - 1$. In 1994 it was proved that, although Carmichael numbers are very rare, there are an infinite number of them [3].

From the perspective of primality testing, a Carmichael number, n, is likely to fail the Fermat Primality Test, because n has only trivial Fermat witnesses, and the number of trivial witnesses is small compared to n, so it is unlikely that we'll find a Fermat witness to n's compositeness, even when the test is run for many rounds.

Summary: The Fermat Primality Test is a classic Monte Carlo algorithm, requiring k rounds, however, there are a few integers n for which it doesn't work well. Given an integer n, if we run the Fermat Primality Test on n for k rounds and no Fermat witness is found, then *either* n is one of the rare Carmichael numbers, *or* n is prime with probability $\geq 1 - 2^{-k}$.

23.4 Miller–Rabin Primality Test

Unlike the Fermat Primality Test, the Miller–Rabin Primality Test works on every number n. Like the Fermat Primality Test, the Miller–Rabin test always returns "prime" if n is prime. For every composite n (including Carmichael numbers), it returns "composite" with probability $> \frac{3}{4}$ in each round. Thus with probability $> 1 - 4^{-k}$ a composite number will be witnessed in k rounds.

23.4.1 A New Witness of Compositeness

The Miller–Rabin test is based on using a new witness of compositeness. We've seen that finding a divisor witness proves n is composite. We've also seen that finding a Fermat witness proves that n is composite. A third way to prove that n is composite is to find a non-trivial square root of 1 mod n. The idea is based on the following theorem.

Theorem 23.11 *If p is prime, then all integer roots of*

$$x^2 \equiv 1 \bmod p$$

satisfy $x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$.

Proof:

$$x^2 \equiv 1 \bmod p \implies p \,\Big|\, \left(x^2 - 1\right)$$
$$\implies p \,|\, (x-1)(x+1).$$

Hence, since p is prime, either $p \mid (x-1)$ or $p \mid (x+1)$ or both.[1] But this says that either $x - 1 \equiv 0 \bmod p$ or $x + 1 \equiv 0 \bmod p$, or both.

This says that the only possible roots are $x \equiv 1 \bmod p$ and $x \equiv -1 \bmod p$. To complete the proof, we note that both these potential roots in fact satisfy the equation $x^2 \equiv 1 \bmod p$. ■

Corollary 23.12 *Given integers n and x, such that* $x^2 \equiv 1 \bmod n$. *If* $x \not\equiv \pm 1 \bmod n$, *then n must be composite.*

Suppose that

$$x^2 \equiv 1 \bmod n. \tag{23.3}$$

We say that $x \equiv \pm 1 \bmod n$ are *trivial* roots of (23.3). By contrast, if $x \not\equiv \pm 1 \bmod n$ satisfies (23.3), then we say that x is a *non-trivial* root of (23.3).

Definition 23.13 *Given a composite number n, we say that x is a* **root witness of *n*'s compositeness** *if* $x^2 \equiv 1 \bmod n$ *and* $x \not\equiv \pm 1 \bmod n$. *A root witness is by definition a* **non-trivial root**.

23.4.2 Logic Behind the Miller–Rabin Test

The Miller–Rabin Primality Test is unintuitive when you hear it, so, rather than just stating it, we will develop it ourselves from scratch. The test attempts to determine that n is composite by looking for one of *two different types of witnesses*, either a Fermat witness *or* a root witness. It is thus much more powerful than the Fermat Primality Test.

We assume $n > 2$, and choose a randomly from $S = \{1, 2, \ldots, n-1\}$. We also assume that n is odd, because if n is even we immediately output "composite."

[1] This follows from the Unique Prime Factorization Theorem (UPFT). UPFT states that every integer $n > 1$ can be written as a unique product of primes:

$$n = p_1^{c_1} \cdot p_2^{c_2} \cdots p_k^{c_k},$$

where the p_i's are distinct primes and the c_i's are non-negative integers. From UPFT, it follows that if $p \mid ab$, then either $p \mid a$ or $p \mid b$, since either a or b (or both) must contain p in its unique factorization.

Given that n is odd, we will consider $n-1$, which must be even.

Since $n-1$ is even, it contains at least one factor of 2. Let's peel off all the factors of 2 in $n-1$. We are left with

$$n-1 = 2^r \cdot d, \tag{23.4}$$

where $r > 0$ is the number of factors of 2 in $n-1$, and d is by definition odd.

The Fermat test tells us that if

$$a^{n-1} \not\equiv 1 \bmod n, \tag{23.5}$$

then a is a Fermat witness of compositeness. By contrast if $a^{n-1} \equiv 1 \bmod n$, then we haven't learned anything, that is, n might still be prime.

We can rewrite (23.5) in terms of r and d, via (23.4), to say that if

$$a^{2^r \cdot d} \not\equiv 1 \bmod n,$$

then we have a Fermat witness of compositeness, so we return "composite" and we're done.

Now suppose instead that:

$$a^{2^r \cdot d} \equiv 1 \bmod n. \tag{23.6}$$

Question: We haven't found a Fermat witness, but is there a test that we can do to look for a root witness?

Hint: Think about (23.6) as a square equation. What is its root?

Answer: Let's rewrite (23.6) as follows:

$$\left(a^{2^{r-1} \cdot d}\right)^2 \equiv 1 \bmod n. \tag{23.7}$$

Now we can ask whether (23.7) has a non-trivial root.

If

$$a^{2^{r-1} \cdot d} \not\equiv \{1, -1\} \bmod n,$$

then we have found a root witness of compositeness, so we return "composite" and we're again done.

Now suppose instead that:

$$a^{2^{r-1} \cdot d} \equiv \{1, -1\} \bmod n.$$

Question: Do we get another chance to try to find a root witness?

Answer: If

$$a^{2^{r-1}\cdot d} \equiv -1 \bmod n, \tag{23.8}$$

there's nothing we can do. In this case we're done testing. Given that we haven't found any witness, we should return "probably prime," and we're done. However, if

$$a^{2^{r-1}\cdot d} \equiv 1 \bmod n, \tag{23.9}$$

and $r - 1 > 0$, then we do in fact get *another chance* to find a root witness of compositeness.

Question: Back in (23.8) we said that if $a^{2^{r-1}\cdot d} \equiv -1 \bmod n$, then we're done. How do we not know that some lower exponent (some future square root) won't give us another opportunity to find a non-trivial square root of 1?

Answer: To witness a non-trivial square root of 1, we need to again experience an equation of the form $x^2 \equiv 1 \bmod n$, where x is some lower power of a obtained by taking future square roots. However, this can't happen. Observe that once we see that some power of a is equivalent to 1 mod n, then all future squares will also be congruent to 1 mod n. So given that $a^{2^{r-1}\cdot d} \equiv -1 \bmod n$, it is impossible that some future square root will be congruent to 1 mod n.

23.4.3 Miller–Rabin Primality Test

Algorithm 23.14 shows a version of the Miller–Rabin algorithm based on our arguments in Section 23.4.2. For simplicity, this is shown for only a *single round*, that is, a single choice of $a \in \{1, 2, \ldots, n-1\}$. In practice, Algorithm 23.14 would be repeated with k different randomly chosen a values. Only if no witness is found in all k iterations do we return a final "probably prime." Otherwise we return "composite."

Algorithm 23.14 (Miller–Rabin Primality Test: Single Round – Take 1)
Given: Integer $n > 2$, where n is odd:

1. *Express $n - 1 = 2^r \cdot d$ for some odd d.*
2. *Choose $a \in \{1, 2, \ldots, n-1\}$ uniformly at random.*
3. *If $a^{2^r \cdot d} \bmod n \not\equiv 1$, return COMPOSITE-Fermat, and stop.*
4. *For $y = r - 1$ to $y = 0$:*
   - *If $a^{2^y \cdot d} \bmod n \not\equiv \{1, -1\}$, return COMPOSITE-Root, and stop.*
   - *If $a^{2^y \cdot d} \bmod n \equiv -1$, return PROBABLY PRIME, and stop.*
   - *(If we get here then we know that $a^{2^y \cdot d} \bmod n \equiv 1$, so we have another chance to find a non-trivial root, assuming $y > 0$.)*
5. *Return PROBABLY PRIME.*

While Algorithm 23.14 is entirely correct, it is more computationally expensive than needed, because it requires first computing $a^{2^r \cdot d}$. This is achieved by starting with a^d and then repeatedly squaring that quantity r times. It is possible to restate Algorithm 23.14 where we compute only those powers of a that are needed. Algorithm 23.15 shows the more efficient version.

Algorithm 23.15 (Miller–Rabin Primality Test: Single Round – Take 2)
Given: Integer $n > 2$, where n is odd:

1. *Express $n - 1 = 2^r \cdot d$ for some odd d.*
2. *Choose $a \in \{1, 2, \ldots, n-1\}$ uniformly at random.*
3. *Let $y = 0$.*
   - *If $a^{2^y \cdot d} \bmod n \equiv 1$, return PROBABLY PRIME, and stop.*
     (Notice all future squares will be 1, so there will be no root witnesses. When we reach $y = r$, the Fermat test will also output probably prime.)
   - *If $a^{2^y \cdot d} \bmod n \equiv -1$, return PROBABLY PRIME, and stop.*
     (Notice that all future squares will be 1 so there will be no root witnesses. When we reach $y = r$, the Fermat test will also output probably prime.)
   - *(If we get here then we still have hope of returning COMPOSITE-Root, if $a^{2^1 \cdot d} \bmod n \equiv 1$.)*
4. *For $y = 1$ to $y = r - 1$:*
   - *If $a^{2^y \cdot d} \bmod n \equiv 1$, return COMPOSITE-Root, and stop.*
   - *If $a^{2^y \cdot d} \bmod n \equiv -1$, return PROBABLY PRIME, and stop.*
     (Notice that all future squares will be 1, so there will be no root witnesses and the Fermat test will return 1 when $y = r$.)
   - *(If we get here then we have the potential for witnessing a root witness if the next round yields a 1.)*
5. *Return COMPOSITE.*

Observe that Algorithm 23.15 will often stop before having to compute all the powers of a.

Question: Why in Algorithm 23.15 did we only go up to $y = r - 1$. Don't we need to check $y = r$ as well? Also, why does the algorithm end by returning "composite"?

Answer: Suppose that we haven't stopped after $y = r-1$. Then it must be the case that $a^{2^{r-1} \cdot d} \not\equiv \{1, -1\} \bmod n$. Now, if $a^{2^r \cdot d} \equiv 1 \bmod n$ we have a root witness, so we should return COMPOSITE-Root. If, on the other hand, $a^{2^r \cdot d} \not\equiv 1 \bmod n$, then we have a Fermat witness and should return COMPOSITE-Fermat. Either way, n is provably composite, so there is no need to check the result of the rth power.

What's shown in Algorithm 23.15 is a single round of the Miller–Rabin Primality

Test. In reality this test is run for k rounds (k instances of a), where the test stops if any round finds a witness of compositeness. If no witness of compositeness is found after k rounds, then the test outputs "probably prime."

As in the case of the Fermat Primality Test, if n is prime, then the Miller–Rabin Primality Test will always output "prime." It can be proven that if n is composite, the Miller–Rabin Primality Test will output composite on a randomly chosen a with probability $> \frac{3}{4}$, for every composite n. This result is due to Michael Rabin and is non-trivial to prove; see [57]. We have chosen to omit the proof because the focus of this book is not on number theory.

Question: If the Miller–Rabin Primality Test is run for k rounds on a composite n, what is the probability that a witness of compositeness is found?

Answer: $> 1 - \left(\frac{1}{4}\right)^k$.

Summary: Recall that the Fermat Primality Test failed on certain composite numbers, the Carmichael numbers, for which very few Fermat witnesses exist. By including a test for a root witnesses, in addition to Fermat witnesses, the Miller–Rabin test improves the probability of witnessing any composite n (including the case where n is Carmichael) all the way to $\frac{3}{4}$. This probability can then be improved with independent runs. Like the Fermat test, the Miller–Rabin test always outputs the correct result when n is prime. Thus there are no numbers on which the Miller–Rabin Primality Test fails to yield a correct result with high probability.

23.5 Readings

For the reader who is interested in reading more on primality testing, with complete proofs, we recommend [30]. In particular, [30, proposition 5.8] provides a proof for why the Miller–Rabin Primality Test is able to detect the compositeness of Carmichael numbers. The proof makes use of some of the unique properties of Carmichael numbers, mentioned earlier.

23.6 Appendix: Proof of Theorem 23.9

Restatement of Theorem 23.9: Let n be composite. Let $S = \{1, 2, \ldots, n-1\}$. Suppose that there exists at least one $a \in S$ such that a is a Fermat witness for n

and $\gcd(a, n) = 1$. Then at least half the elements of S are Fermat witnesses for n.

Proof: [Theorem 23.9] We partition the set S into four disjoint subsets: A, B, C, and D, where

$$\begin{aligned}
A &= \{a \in S \text{ such that } a^{n-1} \equiv 1 \bmod n \quad \text{and} \quad \gcd(a, n) = 1\} \\
B &= \{b \in S \text{ such that } b^{n-1} \not\equiv 1 \bmod n \quad \text{and} \quad \gcd(b, n) = 1\} \\
C &= \{c \in S \text{ such that } c^{n-1} \not\equiv 1 \bmod n \quad \text{and} \quad \gcd(c, n) > 1\} \\
D &= \{d \in S \text{ such that } d^{n-1} \equiv 1 \bmod n \quad \text{and} \quad \gcd(d, n) > 1\}.
\end{aligned}$$

Question: We claim set D is empty. Why is this?

Answer: To see why, suppose integer $k = \gcd(d, n) > 1$. Now suppose also that

$$d^{n-1} \equiv 1 \bmod n.$$

Then, there is some integer q such that

$$d^{n-1} - 1 = q \cdot n.$$

But this is impossible because k divides the term d^{n-1} and also divides the qn term, but k does not divide -1.

Question: Which set is the trivial Fermat witnesses?

Answer: C.

Question: What does set B represent?

Answer: Set B is the non-trivial Fermat witnesses. We're trying to show there are lots of these.

Question: Do we know that sets A, B, and C are all non-empty?

Answer: Yes. Set A must at least contain the number 1. The theorem statement tells us that there is at least one element in B. Set C is non-empty because n is composite.

Restating the theorem statement in terms of these sets, we are trying to show that

$$\text{Given } \exists b \in B, \quad \text{then} \quad |B \cup C| \geq \frac{1}{2}|S|.$$

Let's assume, by contradiction, that $|B \cup C| < \frac{1}{2}|S|$. Then $|A| > \frac{1}{2}|S|$.

We will refer to the elements of A as $\{a_1, a_2, \ldots, a_k\}$, where $k > \frac{1}{2}|S|$.

Now let's take our $b \in B$ and multiply it by all the elements in A, creating the set Ab, which we define as follows:

$$Ab = \{a_1 b \bmod n, \quad a_2 b \bmod n, \quad \ldots, \quad a_k b \bmod n\}.$$

We will now show two properties of the set Ab:

1. $Ab \subset B$.

   To see this, note that every element $j \in Ab$ obeys the three properties needed to be in B. Specifically, if we assume without loss of generality that $j = a_i b \bmod n$, then we have that:
   i. $j^{n-1} \not\equiv 1 \bmod n$.
   (This follows because: $j^{n-1} \equiv (a_i b)^{n-1} \equiv a_i^{n-1} \cdot b^{n-1} \equiv 1 \cdot b^{n-1} \not\equiv 1 \bmod n$.)
   ii. $\gcd(j, n) = 1$
   (This follows because $\gcd(a_i, n) = 1$ and $\gcd(b, n) = 1$, so $\gcd(a_i b, n) = 1$.)
   iii. $j \in S$.
   (By definition j is an integer from 0 to $n-1$. Furthermore, since $\gcd(j, n) = 1$, we known that $j \not\equiv 0 \bmod n$.)

2. The elements of Ab are distinct.

   To see this, suppose by contradiction that

   $$a_i b \bmod n = a_j b \bmod n, \quad \text{where} \quad a_i \neq a_j.$$

   Then $(a_i - a_j)\, b \equiv 0 \bmod n$. So $n \,|\, (a_i - a_j)\, b$. But $\gcd(n, b) = 1$, so it must be the case that

   $$n \,|\, (a_i - a_j)\,. \tag{23.10}$$

   But $a_i < n$ and $a_j < n$ implies that $-n < a_i - a_j < n$, so (23.10) is false, yielding the contradiction.

Properties 1 and 2 together imply that there are at least k elements in B where $k > \frac{1}{2}|S|$. But this is a contradiction. ■

23.7 Exercises

23.1 **Witnesses of compositeness**
Let n be a composite number. Prove that every divisor witness for n is also a gcd witness. Prove that every gcd witness is also a Fermat witness.

23.2 **Fermat test error**
Suppose that $n < 561$, and we are trying to determine whether n is prime or composite. Upper bound the probability of error in the k-round Fermat Primality Test.

23.3 **Number theory reduction**
Prove the following lemma that applies to many statements in this chapter:
Let a, b, c, n be positive integers.
If $ab \equiv ac \bmod n$ and $\gcd(a, n) = 1$, then $b \equiv c \bmod n$.

23.4 **Miller–Rabin**
In the Miller–Rabin algorithm, we are given a number $n > 2$, where n is odd. We express $n - 1$ in the form:

$$n - 1 = 2^r \cdot d.$$

We then pick a random $a \in \{1, 2, 3, \ldots, n-1\}$.
Suppose that we know that $a^{2^{r-1} \cdot d} \not\equiv 1 \bmod n$ and $a^{2^{r-1} \cdot d} \not\equiv -1 \bmod n$.
What does this tell us about n? Choose one answer and explain.
(a) n is prime.
(b) n is composite.
(c) n is composite type Fermat witness.
(d) n is composite type Root witness.
(e) There is insufficient information to deduce any of these.

23.5 **Generating a random prime number**
How can we generate a random prime of value smaller than n with probability larger than $1 - \epsilon$? Consider the following algorithm:

Algorithm 23.16 (Random prime)

1. *Choose an integer r from $\{1, 2, \ldots, n-1\}$ uniformly at random.*
2. *Run the Miller–Rabin test on r for k runs.*
   - *If the test outputs "probably prime" for all k runs, output r as the generated prime and stop.*
   - *If the test outputs "composite" (of any type) in any of the k runs, go back to Step 1.*

In Algorithm 23.16 we say that we are starting a new *"round"* every time we call Step 1. Assume throughout that n is large.
(a) Find an approximate value for k such that the algorithm succeeds with probability larger than $1 - \epsilon$.
(b) Explain why Algorithm 23.16 is not a Las Vegas algorithm.
(c) Explain why Algorithm 23.16 is not a typical Monte Carlo algorithm.
(d) Analyze the expected number of rounds of Algorithm 23.16.