Primality Testing

D.W. Jia *
Department of Mathematics
Stanford University
450 Serra Mall, Stanford, CA 94305

May 29, 2012

Abstract

This paper discusses primality testing: the problem of determining whether a given number is prime or composite. First the paper gives a brief motivational statement to address the importance of testing primality. Next, the paper discusses a particularly useful test of primality called the Miller-Rabin Primality Test. The first section will state the Test. The second section of the paper will provide a formal mathematical proof of correctness for the Miller-Rabin Test. The third section will analyze the randomized aspect of the Test and provide a probability for its the accuracy.

1 Motivation

Primality testing is the problem of determining whether a given number n is prime or composite. Primality testing has tremendous practical purpose. Much of modern cryptography systems depend on large prime numbers as a way of encryption. Primality tests provide an easy way to determine whether a number is prime. Unlike integer factorization, which is a computationally difficult problem, primality testing is relatively non-difficult.

In 1980, Michael Rabin discovered and formalized a randomized polynomial-time algorithm to test whether a number is prime. The algorithm was subsequently named the Miller-Rabin Primality Test because of its close association with a prior deterministic algorithm that was written by Gary Miller in 1976. Till this day, the Miller-Rabin Primality Test is still one of the most practical known primality testing algorithms and is widely used in various software libraries such as OpenSSL that rely on RSA encryption and decryption.

In this paper we will discuss the Miller-Rabin Primality Test. We will give the steps that the test takes, provide a mathematical proof of its correctness, analyze its randomization, and discuss its further implications and corollaries.

2 Miller-Rabin Primality Test

The Miller-Rabin Primality Test as illustrated by the algorithm in Fig 1 (at end of document) can be given in algorithmic form as follows: let $n > 1$ be an odd integer, since n is odd, $n-1$ is even. We can thus write $n - 1 = 2^k m$ for integers m odd and $k \geq 1$. Choose a random integer $a \in \{1, 2, \ldots, n-1\}$ called the base. Then take the following steps:

Step 1: let $b_0 \equiv a^m \mod n$. If $b_0 \equiv \pm 1 \mod n$, then stop and declare that n has passed the test for base a. Otherwise, go to Step 2 with $i = 0$.

Step 2: for $0 \leq i < k-1$, consecutively define $b_{i+1} \equiv b_i^2 \mod n$. For $b_i \not\equiv \pm 1 \mod n$, if $b_{i+1} \equiv 1 \mod n$, then stop and declare that n has failed the test for base a, if $b_{i+1} \equiv -1 \mod n$, then stop and declare that n has passed the test for base a, otherwise if $b_{i+1} \not\equiv \pm 1 \mod n$ and $0 \leq i < k-1$, then let $i \leftarrow i+1$ and repeat Step 2. If $i = k-1$, declare that n has failed the test.

Formally, we define that n passes or fails the test with base a as follows:

Definition 1 (Pass with Base a)**.** For odd integer $n > 1$, we write $n - 1 = 2^k m$ for integers m odd and $k \geq 1$. We choose a random integer $a \in \{1, 2, \ldots, n-1\}$. We say that n *passes the Miller-Rabin Primality Test with base* a if either of the two following conditions holds

$$a^m \equiv 1 \mod n \tag{1}$$

$$a^{2^j m} \equiv -1 \mod n \text{ for some } 0 \leq j \leq k-1 \tag{2}$$

Definition 2 (Fail with Base a)**.** For the same n as defined in Definition 1, we say that n *fails the Miller-Rabin Primality Test with base* a if neither of the conditions (1) or (2) holds.

Remark 1. For a chosen base a, in the case that n fails the test, we conclude that n is composite and that a is a *witness* of n. In the case that n passes the test, we conclude that n is "probably prime".

Remark 2. Note that if for some base a, n passes the test, we can only claims with "high probability" that the tested number n is prime for base a. This means that it is still possible for an integer n to pass the test for certain a and be composite. As we will see later, we call such composite numbers *strong pseudoprimes* because they succeed in the primality test but are nevertheless composite. We will discuss later in this paper what it means to claim with "high probability". But, as we will see, if n is prime, it will always pass the test for any base a. In the opposing case where for some base a, n fails the test, then we can say with probability 1 that the number n is composite. We will prove this fact in the next section.

3 Proof of Correctness

In this section, we provide a formal mathematical proof of correctness for the Miller-Rabin Primality Test for the case given in Definition 2. Namely,

Theorem 1. *If odd composite integer $n > 1$ fails the Miller-Rabin Primality Test with base a, as defined in Definition 2, then n is composite with probability 1.*

*djia@stanford.edu

Before we prove Theorem 1, we give the following intermediary lemma and theorem.

Lemma 1. *If p is a prime and $p > 2$. Let 1 and -1 be the trivial square roots of 1 in modulo p. There are no non-trivial square roots of 1 in modulo p.*

Proof. Suppose that x is a square root of $1 \mod p$. Then $x^2 \equiv 1 \mod p \implies (x-1)(x+1) \equiv 0 \mod p$. This mean that p must divide $(x-1)(x+1)$, but since p is prime, by Euclid's lemma, p must divide one of the factors $x-1$ or $x+1$. This implies that $x-1 \equiv 0 \mod p$, or $x+1 \equiv 0 \mod p$, which directly shows that either $x \equiv 1$ or $x \equiv -1 \mod p$ respectively. □

With the above lemma, we can now give the crucial theorem that proves the correctness of the Miller-Rabin test for an integer n that passes the test with base a.

Theorem 2. *Let $n > 2$ be an odd prime, then $n-1$ is even and we can write $n-1 = 2^k m$ for odd integer m and $k \geq 1$. For every $a \in \{1, 2, \ldots, n-1\}$, either*

$$a^m \equiv 1 \mod n \tag{3}$$

or

$$a^{2^j m} \equiv -1 \mod n \text{ for some } 0 \leq j \leq k-1 \tag{4}$$

Proof. Define the sequence $b_0 \equiv a^m \mod n$ and $b_{i+1} \equiv b_i^2 \mod n$ for all $0 < i \leq k-1$. We divide the proof into two cases:

Case (i) $b_0 \equiv a^m \equiv 1 \mod n$, then we have satisfied the case in (3).

Case (ii) $b_0 \not\equiv 1 \mod n$. We first show that if there exists an i, $1 \leq i \leq k$ such that $b_i \equiv 1 \mod n$, then there must exist a j, $0 \leq j < i$, such that $b_j \equiv -1 \mod n$. Consider, for the sake of contradiction, that for $b_0 \not\equiv 1 \mod n$, there exists an i, $1 \leq i \leq k$ such that $b_i \equiv 1 \mod n$, and for all j such that $0 \leq j < i$, $b_j \not\equiv -1 \mod n$. Then by Lemma 1, $b_j \equiv 1 \mod n$ for all $1 \leq j < i$. This would imply that $b_0 \equiv 1 \mod n$, a contradiction to the assumption that $b_0 \not\equiv 1 \mod n$. So it must be that $b_j \equiv a^{2^j m} \equiv -1 \mod n$ for some $0 \leq j < i$. But since n is prime, by Fermat's Little Theorem, $a^{n-1} \equiv a^{2^k m} \equiv b_k \equiv 1 \mod n$, so there must exist a $1 \leq j < k$ such that $b_j \equiv a^{2^j m} \equiv -1 \mod n$. This gives directly the second condition (4). Thus, one of the conditions must be met. □

Corollary 1. *If n is an odd prime, then it passes the Miller-Rabin Primality Test for all bases $a \in \{1, 2, \ldots, n-1\}$ with probability 1.*

Corollary 1 is self-evident from the proof of Theorem 2 since the conditions for passing the test, (1) and (2), follow directly from conditions (3) and (4) above.

We are now ready for the proof of Theorem 1. It simply tests a number n against the contrapositive of Theorem 2. Now the proof for Theorem 1 is quite simple:

Proof of Theorem 1. Let $n > 1$ be an odd composite integer that fails the Miller-Rabin Primality Test with base a. By Definition 2, this means that there exists an integer $a \in \{1, 2, \ldots, n-1\}$ such that neither of the conditions (3) or (4) are satisfied. Therefore, by the contrapositive of Theorem 2, n is not prime, and thus n is composite. □

Proposition 1. *Let $n > 1$ be an odd integer. Factor $n - 1 = 2^k m$ for m odd and $k \geq 1$. For randomly chosen base $a \in \{1, 2, \ldots, n-1\}$. If $a^m \not\equiv \pm 1 \mod n$, and for some i, $0 \leq i \leq k-1$ we have that $a^{2^i m} \not\equiv \pm 1 \mod n$ and $a^{2^{i+1} m} \equiv 1 \mod n$, then n fails the Miller-Rabin Primality Test with base a.*

Proof. If $a^m \not\equiv \pm 1 \mod n$ then condition (1) is not met. Given this, if for some $1 \leq i \leq k-1$, $a^{2^i m} \not\equiv \pm 1 \mod n$ and $a^{2^{i+1} m} \equiv 1 \mod n$, then for all $0 \leq j \leq i$, $a^{2^j m} \not\equiv -1 \mod n$, otherwise, $a^{2^i m} \equiv \pm 1 \mod n$. Also, since $a^{2^{i+1} m} \equiv 1 \mod n$, then for all $i+1 \leq l \leq k-1$, $a^{2^l m} \equiv 1 \not\equiv -1 \mod n$. This would mean that for no $0 \leq r \leq k-1$, $a^{2^r m} \equiv -1 \mod n$. Therefore, condition (2) is also not met, so by Definition 2, n fails the Miller-Rabin Primality Test with base a. □

Remark 3. Proposition 1 is equivalent to Step 2 of the algorithm of the Miller-Rabin test given in the previous section. This proposition is important because for some values of n, it allows us to declare that n fails the test with base a without necessarily having to calculate (2) for all j. In Fig 1, line 19 illustrates this. This fact allows us to run the the algorithm faster in implementation for some values of n.

Proposition 2. *For an odd composite integer $n > 1$, factor $n - 1 = 2^k m$ for m odd and $k \geq 1$. Given base a, if for some $0 \leq i \leq k-1$, $a^{2^i m} \not\equiv \pm 1 \mod n$ and $a^{2^{i+1} m} \equiv 1 \mod n$ (i.e this will mean that n has failed the Miller-Rabin test), then $\gcd(a^{2^i m} - 1, n)$ and $\gcd(a^{2^i m} + 1, n)$ gives non-trivial factors of n.*

Proof. The equation $a^{2^{i+1} m} \equiv 1 \mod n$ directly implies that $(a^{2^i m})^2 - 1^2 \equiv (a^{2^i m} - 1)(a^{2^i m} + 1) \equiv 0 \mod n$. This means that $(a^{2^i m} - 1)(a^{2^i m} + 1) = rn$ for some positive integer r. Since we know that $a^{2^i m} \not\equiv \pm 1 \mod n$, neither $a^{2^i m} - 1$ nor $a^{2^i m} + 1$ divides n. This implies that $\gcd(a^{2^i m} - 1, n) \neq n$ and $\gcd(a^{2^i m} + 1, n) \neq n$. But any factor of n must also divide the left hand side, so we have that n, which is composite, must share some non-trivial factor with both $a^{2^i m} - 1$ and $a^{2^i m} + 1$. To find these factors we can easily calculate $\gcd(a^{2^i m} - 1, n)$ and $\gcd(a^{2^i m} + 1, n)$ using the Euclidean Algorithm. □

Remark 4. Note that even though Proposition 2 holds, the Miller-Rabin Primality Test does not yield a factoring algorithm. This is because for some bases a such that n fails the test, there does not exist an $0 \leq i \leq k-1$ such that $a^{2^i m} \not\equiv \pm 1 \mod n$ and $a^{2^{i+1} m} \equiv 1 \mod n$. Namely, this happens when n is not a pseudoprime, which we will define in the next section. In this case, we would not be able to apply Proposition 2 and factor n.

4 Likelihood of Failure

We have seen that a number n is composite with probability 1 if the number fails the Miller-Rabin test for some base a, but if the n passes the test for some base a (the test returns "probably prime"), n is only prime with "high probability". In this section, we will give an exact upper bound for the probability that n is composite if it passes the test for a randomly chosen a. In particular, we will show that the following theorem holds:

Theorem 3. *Let n be an odd composite integer, then n will pass the Miller-Rabin Primality Test (output "probably prime") for a randomly chosen base a with probability at most $\frac{1}{4}$.*

Before we give the proof for Theorem 3, we provide the following intermediary steps.

Definition 3 (Pseudoprime Base a)**.** Let n be an odd composite number, call n a *pseudoprime base a* if it satisfies the following condition:

$$a^{n-1} \equiv 1 \mod n \tag{5}$$

Definition 4 (Strong Pseudoprime Base a)**.** Let n be an odd composite number, and write $n-1 = 2^k m$ with m odd, let $b \in \mathbb{Z}_n^*$. Call n a *strong pseudoprime base a* if it satisfies either of the following conditions:

$$a^m \equiv 1 \mod n \tag{6}$$

$$a^{2^j m} \equiv -1 \mod n \text{ for some } 0 \leq j \leq k-1 \tag{7}$$

Proposition 3. *By Definition 4, since (6) and (7) are equivalent to (1) and (2) in Definition 1 respectively, any composite integer n that passes the Miller-Rabin test with base a is a strong pseudoprime base a.*

Proposition 4. *An integer n that is a strong pseudoprime base a is also a pseudoprime base a.*

Proof. If n is a strong pseudoprime base a, then it must satisfy either of the conditions given by (6) and (7). So either $a^m \equiv 1 \mod n$ or for some j, $0 \leq j < k$, $a^{2^j m} \equiv -1 \mod n$. In either case, since 1 and -1 are roots of unity mod n, this must mean that $a^{n-1} \equiv a^{2^k m} \equiv 1 \mod n$. So, by Definition 3, n is a pseudoprime base a. □

Lemma 2. *If $S = \{g, g^2, g^3, \ldots, g^{\phi(n)} \equiv 1\}$ is a cyclic group modulo integer n (where ϕ is the Euler totient function), then there are exactly $d = \gcd(k, \phi(n))$ elements that satisfy $x^k \equiv 1 \mod n$.*

Proof. An element $g^j \in S$ satisfies the equation if and only if $(g^j)^k \equiv g^{jk} \equiv 1 \mod n$, which, by the definition of primitive roots, is true if and only if $\phi(n) | jk$. Given $d = \gcd(k, \phi(n))$, this is true if and only if $\frac{\phi(n)}{d} | j\frac{k}{d}$. Because $\frac{\phi(n)}{d}$ and $\frac{k}{d}$ are relatively prime, $\frac{\phi(n)}{d} \nmid \frac{k}{d}$, so $\frac{\phi(n)}{d} | j$. This is true if and only if j is a multiple of $\frac{\phi(n)}{d}$. There are exactly d such values of j where $1 \leq j \leq \phi(n)$. □

Lemma 3. *Let p be an odd prime, write $p - 1 = 2^{k'} m'$ with m'odd. Then the number of $x \in \mathbb{Z}_p^*$ that satisfies $x^{2^r m} \equiv -1 \mod p$, for m odd, is equal to 0 if $r \geq k'$ and is equal to $2^r \gcd(m, m')$ if $r < m'$.*

Proof. Let g be a generator of $\mathbb{Z}_p^*$. The existence of g is guaranteed by the Primitive Root Theorem. We write x in the form of g^j for $0 \leq j < p-1$. Since $g^{(p-1)/2} \equiv -1 \mod p$ by the definition of primitive roots and Lemma 1, and $p - 1 = 2^{k'} m'$, the congruence given in the lemma is equivalent to solving $2^r m j \equiv 2^{k'-1} m' \mod 2^{k'} m'$ for j. It is clear that for $r > k' - 1$, there is no solutions. If $r \leq k' - 1$, then we can divide out by the gcd of the modulus and the coefficient of the unknown j, which is $2^r d$ where $d = \gcd(m, m')$. Thus, this will give a unique solution to j modulo $2^{k'-r} \frac{m'}{d}$. This means that it has $2^r d$ solutions modulo $2^{k'} m'$, and we have completed the proof of the lemma. □

Proposition 5. *For a composite odd integer n, for at most $\frac{1}{4}$ of all $a \in \{1, 2, \ldots, n-1\}$, n is a strong pseudoprime base a.*

Proof. There are three possible cases for n, we will give the proof for each.

Case (i): n is divisible by the square of some prime p. We have $p^k | n$ for $k \geq 2$. By Proposition 3, if n is not a pseudoprime base a, then n is not a strong pseudoprime base a. So by showing that n cannot be a pseudoprime for more than $\frac{1}{4}$ of the bases a, $0 < a < n$, we will have showed that they also cannot be strong pseudoprimes more than $\frac{1}{4}$ of these bases.

Suppose that for some base a, n is a pseudoprime, then $a^{n-1} \equiv 1 \mod n$. This means $a^{n-1} = mn + 1$ for some positive integer m. Since $p^2 | n$, we take this equation mod p^2 to get

$$a^{n-1} \equiv 1 \mod p^2 \tag{8}$$

So it suffices to find conditions on a such that (8) is true. Note that for this to hold, it must be that $\gcd(a, n) = 1$. Note also that $\mathbb{Z}_{p^2}^*$ (the group formed by the positive integers coprime to and less than p^2) form a cyclic group of order $\phi(p^2) = p^2(1 - \frac{1}{p}) = p(p-1)$. So, by the Primitive Root Theorem (which states that a primitive root exists modulo all powers of a prime p), there exists an integer g such that $\mathbb{Z}_{p^2}^* = \{g, g^2, \ldots, g^{p(p-1)}\}$. By Lemma 2, there are exactly $d = \gcd(n-1, p(p-1))$ integers a that satisfy (8). Because $p(p-1) \leq n-1$, we know that $d \leq p(p-1)$. Since $p | n$ by definition, $p \nmid (n-1)$, so $p \nmid d$. This means that d is at most as large as $p-1$. So the proportion of a, $0 < a < n$ which satisfy 8 is less than or equal to

$$\frac{p-1}{n-1} \leq \frac{p-1}{p^2-1} = \frac{1}{p+1} \leq \frac{1}{4} \tag{9}$$

Note that since n is odd, the smallest possible value of p is 3, which directly gives the right hand side of (10).

Case(ii): n is the product of two distinct primes p and q, so that $n = pq$. We write $p - 1 = 2^{k'} m'$ with m' odd, and $q - 1 = 2^{k''} m''$ with m'' odd. Without loss of generality, we assume that $k' < k''$. For an element $a \in \mathbb{Z}_n^*$ to be a base for which n is a strong pseudoprime, one of the following must be true: (a) $a^m \equiv 1 \mod p$ and $a^m \equiv 1 \mod q$, or (b) $a^{2^r m} \equiv -1 \mod p$ and $a^{2^r m} \equiv -1 \mod q$ for some r, $0 \leq r < k$.

For (a): by Lemma 2, the number of a for such that the case (a) holds is given by $\gcd(m, m') \cdot \gcd(m, m'') \leq m'm''$.

For (b): by Lemma 3, for each $r < \min(k', k'') = k'$, the number of a for which $a^{2^r m} \equiv -1 \mod n$ is $2^r \cdot \gcd(m, m') \cdot 2^r \cdot \gcd(m, m'') < 4^r m'm''$. We have that $n - 1 > \phi(n) = (p-1)(q-1) = 2^{k'+k''} m'm''$. So this directly implies that the fraction of integers $a \in \{1, 2, \ldots, n-1\}$ for which n is a strong pseudoprime is at most

$$\frac{m'm'' + (m'm'' + 4m'm'' + 4^2 m'm'' + \cdots + 4^{k'-1} m'm'')}{2^{k'+k''} m'm''} = 2^{-k'-k''}(1 + \frac{4^{k'} - 1}{4 - 1}) \tag{10}$$

We get the right hand side of (10) by the sum of a geometric series. Since $k'' \geq k'$, either $k'' > k'$ or $k'' = k'$.

If $k'' > k'$, then (10) is at most $2^{-2k'-1}(\frac{2}{3} + \frac{4^{k'}}{3}) \leq 2^{-3}\frac{2}{3} + \frac{1}{6} = \frac{1}{4}$ as we desire.

If $k'' = k'$, then we have that either $\gcd(m, m') \neq m'$ or $\gcd(m, m'') \neq m''$ must be true. This is because if we had $m' | m$ and $m'' | m$, then by the congruence $n - 1 \equiv 2^k m \equiv pq - 1 \equiv q - 1$

mod m', we have that $m'|(q-1) = 2^{k''}m''$, which means $m'|m''$, and by the same logic $m''|m'$. But this means that $m' = m''$ and $p = 1$, a contradiction. So one of the two gcd's is strictly less than m' or m'', and so must be less than by a factor at least 3 since they are odd. So in this case, we can replace $m'm''$ by $\frac{1}{3}m'm''$ in (10). So we have the following upper bound:

$$\frac{1}{3}2^{-2^{k'}}(\frac{2}{3}+\frac{4^{k'}}{3}) \leq \frac{1}{18}+\frac{1}{9} = \frac{1}{6} < \frac{1}{4} \tag{11}$$

Thus we are done with the proof of Case (ii).

Case (iii): n is the product of three or more distinct primes so that $n = p_1p_2\cdots p_l$, where p_i are prime for all i and $p_i \neq p_j$ for $j \neq i$. We write $p_j - 1 = 2^{k_j}m_j$ with m_j odd and take the steps exactly as in Case (ii). Without loss of generality, we assume $k_1 \leq k_j$ for all $j \neq 1$ so that k_1 is the smallest k_j. Since for Case (iii), $l \geq 3$, we obtain in a similar fashion to Case (ii) the following upper bound for the fraction of $a \in \{1, 2, \ldots, n-1\}$ for which n is a strong pseudoprime:

$$2^{-k_1-k_2-\cdots-k_l}(1+\frac{2^{lk_1}-1}{2^l-1}) \leq 2^{-lk_1}(\frac{2^l-2}{2^l-1}+\frac{2^{lk_1}}{2^l-1}) =$$

$$= 2^{-lk_1}\frac{2^l-2}{2^l-1}+\frac{1}{2^l-1} \leq 2^{-l}\frac{2^l-2}{2^l-1}+\frac{1}{2^l-1} = 2^{1-l} \leq \frac{1}{4} \tag{12}$$

Thus we have proved Proposition 5.

□

We are now ready to give the proof of Theorem 3:

Proof of Theorem 3. If an odd composite integer n passes the Miller-Rabin test for a particular base a, then by Proposition 3, this means that n is a strong pseudoprime base a. Proposition 5 states that there cannot be more than $\frac{1}{4}$ of these bases a, $0 < a < n$, for which n is a strong pseudoprime. Thus, since the Miller-Rabin Primality Test chooses a random a, $0 < a < n$, the probability of choosing an a that passes the test for n composite is at most $\frac{1}{4}$ □

Corollary 2. *For odd integer $n > 1$, if n passes the Miller-Rabin Primality Test for r iterations, i.e. r randomly selected bases, then the probability that n is composite is at most $(\frac{1}{4})^r$.*

Remark 5. Theorem 3 and Corollary 2 directly implies that if n passes the Miller-Rabin test for a certain base, the more times we run the test, the less likely the error.

Remark 6. The Miller-Rabin Primality test takes $O(\log n)$ multiplications to complete. These multiplications are required to obtain a^m for a base a. It then takes at most $O(\log n)$ time to compute $a^{2^j m}$ for $1 \leq j \leq k$. Given that mod-n multiplication takes $O(\log^2 n)$ time, the total running time of the test is $O(\log^3 n)$. If we run the test r times, the test takes $O(r \log^3 n)$. Thus, the Miller-Rabin Primality test is in polynomial time with respect to $\log n$, and is efficient for most purposes.

5 Conclusion

In this paper, we have given the algorithm for the Miller-Rabin Primality Test, which is a randomized polynomial time algorithm for testing whether an integer n is prime or composite. With randomly chosen base a, we have shown that when an integer n fails the test, it is composite with probability 1, and when n passes the test, it is prime with probability at least $\frac{3}{4}$. In the case that n passes the test, we can perform the test multiple times for the same n. For randomly chosen a this guarantees that our probability of error is at most $(\frac{1}{4})^r$ where r is the number of times we repeat the test on n. Because of it's polynomial run-time and accuracy, the Miller-Rabin Primality Test remains one of the most widely used primality tests.

References

[1] N. Koblitz *A Course in Number Theory and Cryptography* 2nd ed. (1994)

[2] W. Trappe, L.C. Washington *Introduction to Cryptography with Coding Theory* 2nd ed.

[3] P. Garrett *Making, Breaking Codes: Introduction to Cryptology* (2001)

```
1: function MillerRabin(n, r)
2:     if n > 2 and n is even then
3:         return composite
4:     end if
5:     /* find k and m such that n − 1 = 2^k m for integers k ≥ 1 and m odd. */
6:     k ← 0
7:     m ← n − 1
8:     while m is even do
9:         k ← s + 1
10:        m ← m/2
11:    end while
12:    for j ∈ {1, 2, . . . , r} do
13:        Choose a ∈ {1, 2, . . . , n − 1} uniformly at random.
14:        Compute each value of the sequence {a^m, a^{2m}, a^{2^2 m} . . . a^{2^{k−1} m}}  mod n
15:        if a^m ≡ ±1  mod n then
16:            continue
17:        end if
18:        for i ∈ {1, 2, . . . , k − 1} do
19:            if a^{2^i m} ≡ 1  mod n then
20:                return composite
21:            else if a^{2^i m} ≡ −1  mod n then
22:                break
23:            end if
24:        end for
25:        if a^{2^k m} ≡ a^{n−1} ≢ 1  mod n then
26:            return composite
27:        end if
28:    end for
29:    return probably prime
30: end function
```

Figure 1: The Algorithm for the Miller-Rabin Primality Test on integer n for r cycles, recreated by the author.