Fermat Primality Test

One primality test is based on Fermat's Little Theorem, Theorem (6.3.2).

Fermat Primality Test
Input: prime candidate $\tilde{p}$ and security parameter s
Output: statement "$\tilde{p}$ is composite" or "$\tilde{p}$ is likely prime"
Algorithm:

1 FOR $i = 1$ TO s
1.1 choose random $a \in \{2, 3, \ldots, \tilde{p} - 2\}$
1.2 IF $a^{\tilde{p}-1} \not\equiv 1$
1.3 RETURN ("$\tilde{p}$ is composite")
2 RETURN ("$\tilde{p}$ is likely prime")

The idea behind the test is that Fermat's theorem holds for all primes. Hence, if a number is found for which $a^{\tilde{p}-1} \not\equiv 1$ in Step 1.2, it is certainly not a prime. However, the reverse is not true. There could be composite numbers which in fact fulfill the condition $a^{\tilde{p}-1} \equiv 1$. In order to detect them, the algorithm is run s times with different values of a.

Unfortunately, there are certain composite integers which behave like primes in the Fermat test for many values of a. These are the *Carmichael numbers*. Given a Carmichael number C, the following expression holds for all integers a for which $\gcd(a, C) = 1$:

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

Such special composites are very rare. For instance, there exist approximately only $100,000$ Carmichael numbers below 10^{15}.

Example 7.8. Carmichael Number
$n = 561 = 3 \cdot 11 \cdot 17$ is a Carmichael number since

$$a^{560} \equiv 1 \bmod 561$$

for all $\gcd(a, 561) = 1$.
◇

If the prime factors of a Carmichael numbers are all large, there are only few bases a for which Fermat's test detects that the number is actually composite. For this reason, in practice the more powerful Miller–Rabin test is often used to generate RSA primes.

Miller–Rabin Primality Test

In contrast to Fermat's test, the Miller–Rabin test does not have any composite numbers for which a large number of base elements a yield the statement "prime". The test is based on the following theorem:

> **Theorem 7.6.1** *Given the decomposition of an odd prime candidate* $\tilde{p}$
>
> $$\tilde{p} - 1 = 2^u r$$
>
> *where* r *is odd. If we can find an integer* a *such that*
>
> $$a^r \not\equiv 1 \bmod \tilde{p} \qquad \text{and} \qquad a^{r2^j} \not\equiv \tilde{p} - 1 \bmod \tilde{p}$$
>
> *for all* $j = \{0, 1, \ldots, u-1\}$*, then* $\tilde{p}$ *is composite. Otherwise, it is probably a prime.*

We can turn this into an efficient primality test.

Miller–Rabin Primality Test
Input: prime candidate $\tilde{p}$ with $\tilde{p} - 1 = 2^u r$ and security parameter s
Output: statement "$\tilde{p}$ is composite" or "$\tilde{p}$ is likely prime"
Algorithm:

1 FOR $i = 1$ TO s
  choose random $a \in \{2, 3, \ldots, \tilde{p} - 2\}$
1.2 $z \equiv a^r \bmod \tilde{p}$
1.3 IF $z \not\equiv 1$ and $z \not\equiv \tilde{p} - 1$
1.4   FOR $j = 1$ TO $u - 1$
      $z \equiv z^2 \bmod \tilde{p}$
      IF $z = 1$
        RETURN ("$\tilde{p}$ is composite")
1.5   IF $z \neq \tilde{p} - 1$
      RETURN ("$\tilde{p}$ is composite")
2 RETURN ("$\tilde{p}$ is likely prime")

Step 1.2 is computed by using the square-and-multiply algorithm. The IF statement in Step 1.3 tests the theorem for the case $j = 0$. The FOR loop 1.4 and the IF statement 1.5 test the right-hand side of the theorem for the values $j = 1, \ldots, u-1$.

It can still happen that a composite number $\tilde{p}$ gives the incorrect statement "prime". However, the likelihood of this rapidly decreases as we run the test with several different random base elements a. The number of runs is given by the security parameter s in the Miller–Rabin test. Table 7.2 shows how many different values a must be chosen in order to have a probability of less than 2^{-80} that a composite is incorrectly detected as a prime.

Table 7.2 Number of runs within the Miller–Rabin primality test for an error probability of less than 2^{-80}

Bit lengths of $\tilde{p}$	Security parameter s
250	11
300	9
400	6
500	5
600	3

Example 7.9. Miller–Rabin Test

Let $\tilde{p} = 91$. Write $\tilde{p}$ as $\tilde{p} - 1 = 2^1 \cdot 45$. We select a security parameter of $s = 4$. Now, choose s times a random value a:

1. Let $a = 12$: $z = 12^{45} \equiv 90 \bmod 91$, hence, $\tilde{p}$ is likely prime.
2. Let $a = 17$: $z = 17^{45} \equiv 90 \bmod 91$, hence, $\tilde{p}$ is likely prime.
3. Let $a = 38$: $z = 38^{45} \equiv 90 \bmod 91$, hence, $\tilde{p}$ is likely prime.
4. Let $a = 39$: $z = 39^{45} \equiv 78 \bmod 91$, hence, $\tilde{p}$ is composite.

Since the numbers 12, 17 and 38 give incorrect statements for the prime candidate $\tilde{p} = 91$, they are called “liars for 91”.

$\diamond$