4.2.3 Miller-Rabin test

The probabilistic primality test used most in practice is the Miller-Rabin test, also known as the *strong pseudoprime test*. The test is based on the following fact.

4.20 Fact Let n be an odd prime, and let $n-1 = 2^s r$ where r is odd. Let a be any integer such that $\gcd(a,n) = 1$. Then either $a^r \equiv 1 \pmod{n}$ or $a^{2^j r} \equiv -1 \pmod{n}$ for some $j, 0 \le j \le s-1$.

Fact 4.20 motivates the following definitions.

4.21 Definition Let n be an odd composite integer and let $n-1 = 2^s r$ where r is odd. Let a be an integer in the interval $[1, n-1]$.

(i) If $a^r \not\equiv 1 \pmod{n}$ and if $a^{2^j r} \not\equiv -1 \pmod{n}$ for all $j, 0 \le j \le s-1$, then a is called a *strong witness* (to compositeness) for n.

(ii) Otherwise, i.e., if either $a^r \equiv 1 \pmod{n}$ or $a^{2^j r} \equiv -1 \pmod{n}$ for some $j, 0 \le j \le s-1$, then n is said to be a *strong pseudoprime to the base* a. (That is, n acts like a prime in that it satisfies Fact 4.20 for the particular base a.) The integer a is called a *strong liar* (to primality) for n.

4.22 Example (*strong pseudoprime*) Consider the composite integer $n = 91$ $(= 7 \times 13)$. Since $91 - 1 = 90 = 2 \times 45$, $s = 1$ and $r = 45$. Since $9^r = 9^{45} \equiv 1 \pmod{91}$, 91 is a strong pseudoprime to the base 9. The set of all strong liars for 91 is:

$$\{1, 9, 10, 12, 16, 17, 22, 29, 38, 53, 62, 69, 74, 75, 79, 81, 82, 90\}.$$

Notice that the number of strong liars for 91 is $18 = \phi(91)/4$, where ϕ is the Euler phi function (cf. Fact 4.23). □

4.23 Fact If n is an odd composite integer, then at most $\frac{1}{4}$ of all the numbers a, $1 \le a \le n-1$, are strong liars for n. In fact, if $n \ne 9$, the number of strong liars for n is at most $\phi(n)/4$, where ϕ is the Euler phi function (Definition 2.100).

4.24 Algorithm Miller-Rabin probabilistic primality test

MILLER-RABIN(n,t)
INPUT: an odd integer $n \ge 3$ and security parameter $t \ge 1$.
OUTPUT: an answer "prime" or "composite" to the question: "Is n prime?"

1. Write $n - 1 = 2^s r$ such that r is odd.
2. For i from 1 to t do the following:
   2.1 Choose a random integer a, $2 \le a \le n-2$.
   2.2 Compute $y = a^r \bmod n$ using Algorithm 2.143.
   2.3 If $y \ne 1$ and $y \ne n-1$ then do the following:
         $j \leftarrow 1$.
         While $j \le s-1$ and $y \ne n-1$ do the following:
            Compute $y \leftarrow y^2 \bmod n$.
            If $y = 1$ then return("composite").
            $j \leftarrow j+1$.
         If $y \ne n-1$ then return ("composite").
3. Return("prime").

Algorithm 4.24 tests whether each base a satisfies the conditions of Definition 4.21(i). In the fifth line of step 2.3, if $y = 1$, then $a^{2^j r} \equiv 1 \pmod{n}$. Since it is also the case that $a^{2^{j-1} r} \not\equiv \pm 1 \pmod{n}$, it follows from Fact 3.18 that n is composite (in fact $\gcd(a^{2^{j-1} r} - 1, n)$ is a non-trivial factor of n). In the seventh line of step 2.3, if $y \ne n-1$, then a is a strong witness for n. If Algorithm 4.24 declares "composite", then n is certainly composite because prime numbers do not violate Fact 4.20. Equivalently, if n is actually prime, then the algorithm always declares "prime". On the other hand, if n is actually composite, then Fact 4.23 can be used to deduce the following probability of the algorithm erroneously declaring "prime".