Miller-Rabin primality test.

We describe an improved version of Fermat's primality test.

Let n be an odd number, which we want to test and see whether it is prime. Here is the algorithm.

Step 1. Write n in the form $n = 2^s \cdot l + 1$, so that l is odd.

Step 2. Choose $a \in \mathbb{Z}_n$, $a \neq 0$. If $a^{2^s \cdot l} \not\equiv 1$, n is not prime.

Otherwise, for $k \in \{1, \dots, s\}$:

check if $a^{2^{s-k} \cdot l} \equiv \pm 1 \pmod n$

if it is not, break the cycle, n is not prime;

if $a^{2^{s-k} \cdot l} \equiv -1$, break and choose a different a;

if $a^{2^{s-k} \cdot l} \equiv 1$, increase k and repeat.

Def-n. Let $n = 2^s \cdot l + 1$ be an odd number (l is odd). An integer a with $\gcd(a, n) = 1$ is called a Miller-Rabin witness for (the compositeness of) if: • $a^{n-1} \not\equiv 1$;

elif: • $a^{2^k l} \not\equiv \pm 1$ for all $k \in \{1, 2, \dots, s-1\}$;

elif: • $a^l \not\equiv 1$.

If n is composite and the chosen a is not a witness of that, then a is called a (strong) liar.

Prop-n. Let $n \in \mathbb{Z}_{>0}$ be an odd composite number. Then $\geq 75\%$ of the numbers $\{1, 2, \dots, n-1\}$ are Miller-Rabin witnesses of compositeness of n.

Corollary. The probability that k chosen numbers are strong liars does not exceed $\frac{1}{4^k}$, e.g. the chance that n is composite, but we do not find that out after trying 5 different a's is $\leq \frac{1}{4^5} \approx 6 \cdot 10^{-5}$.

Facts: if $n < 2047$, it is enough to test for $a = 2$;
if $n < 1.373.653$, it is enough to test for $a = 2$ & 3;
if $n < 3.215.031.751$, it is enough to test for $a = 2, 3, 5, 7$.

Example. Recall that Fermat's primality test 'failed' to distinguish Carmichael's numbers as composite. These are numbers n, s.t. $\forall a \in \mathbb{Z}_n$, $\gcd(a, n) = 1$ we have $a^{n-1} \equiv 1 \pmod{n}$. The first such number was found by Carmichael (the definition is due to Korselt). This number is $n = 561$, it is the smallest Carmichael number.

Let's run Miller-Rabin test for this number.

Step 1. $n = 561 = 2^4 \cdot 35 + 1$.

Step 2. Choose $a = 2$.

$$2^{560} \equiv 1 \pmod{561}$$

$$2^{2^3 \cdot 35} \equiv 2^{280} \equiv 1 \pmod{561}$$

$$2^{2^2 \cdot 35} \equiv 2^{140} \equiv 67 \not\equiv \pm 1 \pmod{561}.$$

Hence, $a = 2$ is a witness for $n = 561$ and the number is composite.