

Of course, we could have been unlucky with the random pick

$$\text{ex: } a \equiv 8 \quad 8 \equiv -1 \pmod{9}$$
$$8^8 \equiv (-1)^8 \equiv 1 \pmod{9}$$

8 passes the test

When you pick a random a which passes the test, then try again with a different a (probabilistic primality test). The probability of passing the test multiple times when n is not prime is (usually) very low.

More precisely, the probability that a passes the test is (most of the time) $< \frac{1}{2}$

Repeat test 10 times:

\Rightarrow Probability of passing the test 10 times when n is not prime $\leq \frac{1}{2^{10}} < \frac{1}{1000}$

\Rightarrow with high probability, n is prime

There are catches:

Definition: a Fermat Pseudoprime (or Carmichael number) is a number n such that, for $1 \leq a < n$

$$\gcd(a, n) = 1 \Rightarrow a^{n-1} \equiv 1 \pmod{n}$$

ex: 561, 1105, 1729, 2465

Good news; those numbers are rare, and for all other non prime numbers, the probability is $< \frac{1}{2}$

Last year, a high school student (Daniel Larson) proved a 30 years old conjecture about the distribution of those numbers

$\forall x$ large enough, $\exists c$ pseudoprime $x < c < 2x$