Miller–Rabin Primality Testing

Probabilistic Computing

Ben Burger

2020-11-12

Fermat's Theorem

If n if prime, then for any a, we have $a^{n-1} = 1(\text{mod} n)$

This suggests the Fermat test: pick a random $a \in [1..n-1]$ and see if $a^{n-1} = 1(\text{mod} n)$ holds.

Miller-Rabin Theorem

We recall that n is prime if and only if the solutions of $x^2 = 1(\text{mod} n)$ are $x = \pm 1$.

If n passes the Fermat test, we should also check $a^{(n-1)/2} = /\text{pm}1$.

Similarly, the Miller-Rabin test picks a random $a \in [1..n-1]$ and determines if these equalities hold.

Performance

Methodology

Test Primality

Checks base case, calls the Miller-Rabin test k times.

Miller-Rabin

Chooses a random a value, performs Miller-Rabin test.

Power

Modular exponentiation utility function.