

Primality Tester

N: 29

K: 10

Test Primality

Fermat Result: 29 is prime with probability 0.999023437500000

MR Result: 29 is prime with probability 1.000000000000000

1. ^^
2. ATTACHED
3. I did all the time complexity as commented on each function in the code.
4. 2 EQUATIONS:

For Fermat, we know that if a number is Prime, all of the numbers below it will have a mod 1 when you put it up to the mod_exp. This is because every number is relatively prime to a prime number, and you can prove that it will not be anything BUT mod 1 when you put up any number $a^{N-1} \equiv 1 \pmod{N}$.

When we looked at the 2 equations, we knew that Fermat had a 50% probability for each random number called underneath it to be correct. Since for numbers that are NOT prime, 1/2 of the numbers below them will pass a single Fermat test with the NOT prime number aforementioned. With this being noted, we knew that for each call of Fermat with a prime number, every time it came back true increased the probability by 50%; so if we had 3 tests, our probability was 87.5% that it was prime IF they all came back positive. The more tests you run, the higher the probability is.

For the Miller Rabin equation, it is a bit more complicated, as it uses more time complexity, but the guarantee you have a prime number is drastically higher than Fermat. If you have a prime number, and you test the Mod_Exp of $(a, N-1, N)$ with "a" being a random number below the testing prime number, if this comes back 1, you haven't proven anything yet. IF the exponent is even, and you divide it in 2, and run it through Mod_Exp again, and it comes back a 1, or -1, it increases the odds that you have found a prime number not by 1/2, but by 99999/100000!

When we looked at Miller Rabin, we found that the book said that for each test you run for a NOT prime number, the probability of it passing one test where you cut the even exponent in half came out to be 1/100000. I did not understand how this statistic makes sense, but whenever we would run a single test, it came back accurate every time whether it was prime or NOT prime. This lead us to believe that probability was correct. So for each number of tests we ran, our probability we had a real prime number increased by 99999/100000x.