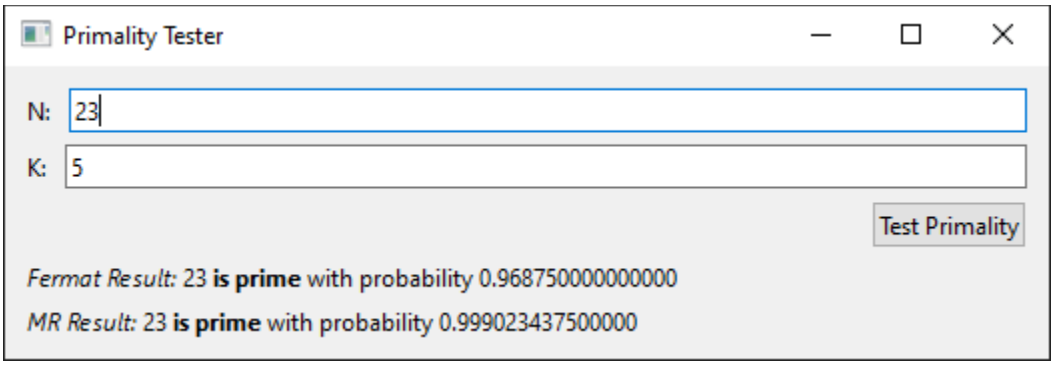
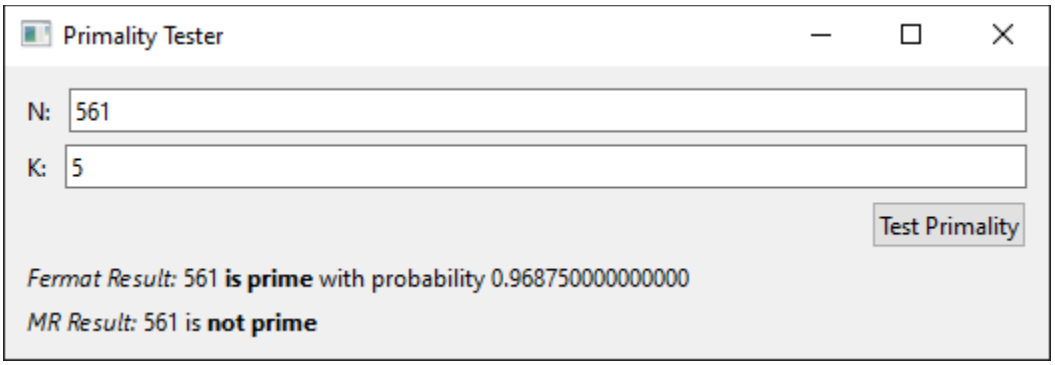


The text explained that Carmichael numbers, like 561, can trick the Fermat test because a^{N-1-} mod(N) = 1 for values relatively prime to N. I personally found that if the test used an a that was a multiple of 3 that it would still catch 561, because they are not relatively prime to 561, but since it tricks the test for relatively prime values, it can trick the algorithm for lower values of K



The Fermat test has complexity k*log(n) where k is the number of iterations, because each iteration has to do modular exponentiation, which is log(n) complexity

The Miller Rabin test has $k*\log(n)^2$ complexity, because the first loop runs k times, and the second loop runs t times, and the max value of t is $\log_2 n$. Inside the inner loop it does modular exponentiation which has log(n) complexity.

I determined the correctness probability of the fermat test using this formula from the book
Pr(Algorithm 1.8 returns yes when *N* is not prime) $\leq 1/2^k$
S the chance that k consecutive tests will be incorrect is $.5^k$, making the probability of it being correct $1-.5^k$

The Miller Rabin test will identify a composite number at least 3/4s according to the text, so the chance that k consecutive tests will be fail to do so is $.25^k$, making the probability of correctly identifying a composite number $1-.25^k$