1. The probability of the output being actually prime is the “probability of output is actually prime *given* that Rabin-Miller-k says it’s ‘probably prime’”. Let denote the event that “Rabin-Miller-k says N is ‘probably prime’” and denote the event that “ *is* prime”. The problem is now formally to show .

Baye’s Rule:

Use it:

The Total Probability Rule:

Use it to rewrite :

( means the complement of , so, “ is composite”.)

Bringing it all together:

Multiply by :