**Miller - Rabin Primality Testing**

Shubho

Sep 2, 2015, 6:29 PM

[Previously Published Here](https://sites.google.com/site/vinceandcode/number-theory/miller---rabin-primality-testing)

|  |
| --- |
| <http://news.harvard.edu/gazette/2004/12.16/photos/4-rabin1-450.jpg>  Miller - Rabin test is not 100% accurate all the time.  **Basic principle :**   if x^2 is congruent to y^2(mod n) where x is not congruent to y (+ or - ) (mod n) then n is a  composite number.  **Things we need**  1.    n-1 = 2^k \* m;  2.    1<a<n-1;  3.   b0 = a^m (mod n); b1  =  b0 ^2,....  (if 3 results in congruent +1 then the number is composite, if -1 then the number maybe is prime)  **Example:**  let's say our n = 561;  is it prime or not?     561-1 =  2^k \* m;      560/2^1 = 280      560/2^2 = 140      560/2^3 = 70      560/2^4 = 35      560/2^5 = 17.5// now here we are getting a fraction so we will consider                               the calculation above.  so k = 4 and m = 35;  561 = 2^4 \* 35;  let's say a = 2;  b0 = 2^35 (mod 561) = 263 (mod 561);   b1  = b0 ^2 = 166 (mod 561);   b2  = b1^2 = 67 (mod 561);   b3 = b2^2 = 1 (mod 561) // we got positive 1 so the number is composite.    Note 561 is a carmichael number |