FERMAT TEST AND THE EXISTENCE OF PSEUDOPRIMES

Ega Gradini [1]

ABSTRACT

In this paper the author present Fermat test as one of primality tests. In order to perform the ability of the test, the algorithm of the test coded in Mathematica (6.0 version). The application of Fermat's Little Theorem as well as Euler's Theorem on the tests are also discussed and this leads to the concept of pseudoprime.

Keywords: *Fermat Test, Mathematica*

[1] Ega Gradini, Dosen Prodi Pendidikan Matematika – STKIP Bina Bangsa Getsempena Banda Aceh, Jalan Tgk Chik Di Tiro, Peuniti Banda Aceh, Telepon 0651-33427, Email: ega@stkipgetsempena.ac.id

INTRODUCTION

Issue of security is the most common issue in human life. Almost all activities involve security issue such as Personal Identification Number (PIN) of ATM, electronic mail, purchase good with credit card, fund transfer, even an order to have war from the armies of a country to another. Companies, government and individuals need to send messages in a way where only the intended recipient able to read the message. Prime number plays an important role in the RSA (Rivest, Shamir & Adler) cryptography. Until now, there is no valid formula to produce prime number, one of the recent technologies is to determine primality or compositeness of an integer given.

Primality test is the process to testing whether a given integer *n* is a prime or not. There are two types of primality tests: deterministic and probabilistic. Deterministic test is primality test that determine with absolute certainty whether a number is prime or not. Lucas-Lehmer test is one of the deterministic primality tests. Probabilistic test also determine whether a given number *n* is a prime or not, but probabilistic test can potentially (although with very small probability) falsely identify a composite number as prime (not vice versa). However, they are in the general much faster than deterministic test. Fermat test, Solovay-Strassen test, and Miller-Rabin test are some of probabilistic primality test.

In this project Fermat test was being carried out using the help of *Mathematica 6.0* software to assess the ability. *Mathematica 6.0* is very easy to learn and the command is very simple. *Mathematica 6.0* has so many build-in functions that can carry out many technical tasks like counting digit number, solving congruency and modulo problems, where this function is so much needed in carrying out the tests that we will see later. *Mathematica 6.0* also has a build-in function to count number of primes less than an integer and many more functions related to number theoretical concept.

Fermat test are probabilistic tests since they cannot certainly identify the given number is prime, sometimes they fail. This is due to the Fermat's little theorem and Euler's theorem which does not work in both ways [Jones].

Fermat Little Theorem says that if *n* is a prime then

$an \equiv a \pmod{n}$. Euler's Theorem also says that If *p* is a prime number and *a* is an integer, then

$a^p \equiv a \pmod{p}$. Furthermore, if the greatest common divisors of *a* and *p* is 1, then

$a^{(p-1)} \equiv 1 \pmod{p}$ (Mcintosh, 2007).

These theorems do not guarantee the primality of *n* even if *n* satisfies the congruency. Therefore these theorems do not work in both ways but the tests assumed

that it works. That is why pseudoprime exists. The source code of each test using Mathematica 6.0 is shown in section 2.
In section 3, the pseudoprime is discussed, including Carmichael numbers as absolute pseudoprime.

A. Fermat Test and the Coding In *Mathematica 6.0* Software

The following source codes are derived from an algorithm obtained mainly from Fermat's theorem, Euler's Theorem and other related theorems from number theory to test whether or not the given number is a prime number. First, first 100 integers set as the input. The output will come up as a prime or a composite. After this is done the author enlarge the input range to the first 1000 and until 10,000. The author shows the source codes here as they are the main task for this project. The author also used some build-in functions of *Mathematica 6.0* to carry out some technical tasks, like finding the exact number of primes less than an integer, tabulating prime numbers, pseudoprimes, and Carmichael numbers obtained from the output of the following source codes, drawing and plotting facilities are also been used to facilitate our tasks. The build-in *Mathematica 6.0* commands, "PrimeQ[*integer*]" and "PrimePi[*integer*] are used to compare the list of primes and pseudoprimes and to compute percentage of pseudoprimes produced by each test. To get a full picture of this project, the author suggest one refers to (Gradini, 2009).

2.1 Prime Number Theorem

Let $\pi(x)$ denote the number of prime number $\leq x$. Then for large values of x, $\pi(x)$ is closely approximated by the x (Bektas, 2005).

By using built-in program in *Mathematica* (6.0 version), we can get the number of prime number $\leq x$, is denoted as $n(x)$. In the table below, we list down the number of prime number $\leq x$ by using Theorem 2.3.1 and built-in program in *Mathematica* (6.0 version).

Table 2.1 List of $\pi(x)$, $x \leq$ 10,000,000,000 by theorem 2.3.1

x	x
10	4
100	22
1,0000	145
10,0000	1,086
100,0000	8,686
1,	72,383

0 0 0 0 , 0 0 0 0	
1 0 , 0 0 0 0 , 0 0 0 0	620,421
1 0 0 , 0 0 0 , 0 0 0 0	5,428,682
1 , 0 0 0 , 0 0 0 , 0 0 0 0	48,254,943
1 0 , 0 0 0 , 0 0 0 , 0 0 0 0	434,294,482

Table 2.2 List of $n(x)$, $x \leq 10{,}000{,}000{,}000$ by using *Mathematica (6.0 version)*.

x	$n(x)$
10	4
100	25
1,000	168
10,000	1229
100,000	9592
1,000,000	78498
10,000,000	664579
100,000,000	5761455
1,000,000,000	50,847,534
10,000,000,000	455,052,511

It can be seen there are some differences between number of prime number approximated by theorem with the result *Mathematica* (6.0 version) given. Later, in computation, Table 2.2 will be used as the exact number of prime.

2.2 Fermat Little Theorem

Pierre de Fermat (1601-1665) is one of the most famous mathematicians in the world since his works on number theory, algebra, calculus, probability and analytic geometry. His most famous work is Fermat little theorem and Fermat last theorem, which is Fermat little theorem become one of the fundamental theory in primality testing.

Theorem 2.2.1 Fermat Little Theorem

If p is a prime number and a is an integer, then $a^p \equiv a \pmod{p}$. Furthermore, if the greatest common divisors of a and p is 1, then $a^{(p-1)} \equiv 1 \pmod{p}$ (Mcintosh, 2007). Proofs of the theorem can be found in any algebra text, here is one of them.

Proof: Consider the first $p-1$ positive multiples of a, that is, the integer $a, 2a, 3a, \ldots, (p-1)a$. None of this number is congruent modulo p to neither any other nor zero. If it happened

$$ra \equiv sa \pmod{p},\ 1 \le r < s \le p-1$$

then a could be cancelled to gives $r \equiv s \pmod{p}$, which is impossible. Therefore, the previous set of integer must be congruent modulo p to 1, 2, 3, …, $p-1$, taken in some order. Multiplying all these congruent together, we find that

$$a.2a.3a\ldots(p-1)\,a \equiv 1.2.3\ldots.(p-1) \pmod{p}$$

then

$$a^{(p-1)}(p-1)! \equiv (p-1)! \pmod{p}$$

by cancelling $(p-1)!$ from both sides of the preceding congruence, this is possible since $p \nmid (p-1)!$, gives $a^{(p-1)} \equiv 1 \pmod{p}$ (Dorsey, 1999).

Fermat's theorem allows proving that a given number n is composite without factoring it. Fermat's little theorem can be change in alternate statement, if $a^{(n-1)} \not\equiv 1 \pmod{n}$ for some a with $a \not\equiv 0 \pmod{n}$ then n is composite.

Lemma 2.2.1

If $2^m + 1$ is prime, then $m = 2^n$ for some integer $n \ge 0$ (Eynden, 2001).

There is a mistake among Fermat works, he $n+1$, $n \ge 0$ prime, thus he has a formula to perform prime value. But then, some mathematicians disapproved Fermat conjecture. According to Yan (2000), here are some of them:

5+ 1, was factored by Euler in 1732 by showing that

32+ 1 = 641.6700417

6+1 was factored by Landry and

$6+1 = 2^{64} + 1 =$ 274177.67280421310721

7+ 1 was factored by Brent and Pollard in 1980 by using Brent and Pollard's Monte Carlo (rho)

$7+1 = 2^{256} + 1 =$ 1238926361552897. ρ_{63}

9+1 was factored by Lenstra *et al*. in 1990 by using Number Field

$9+1 = 2^{512} + 1 =$ 2424833.74556028256478842083373957362004549187833663426 57. ρ_99

Definition 2.2.1

A composite number n is a pseudo-prime to base a (psp(a) or a-pseudo-prime) if $a^n \equiv a \pmod{n}$. Note that, if GCD (a, n) = 1, the condition above is equivalent

with $a^{n-1} \equiv 1 \pmod{n}$ (Kumanduri and Romero, 1998).

2.3 Fermat Test

Fermat test is developed from Fermat Little Theorem and then become one of the probabilistic prime testing. According to Fermat's Little Theorem, if *n* is prime and GCD (*a*, *n*) = 1 then $a^{n-1} \equiv 1 \pmod{n}$. If *n* is not prime, it is not necessary true that $a^{n-1} \equiv 1 \pmod{n}$, but there still a possibility.

According to Herman and Soltys (2008), all primes pass the Fermat test for all $a \in \mathbb{Z}$. Fermat's theorem also can be used to test compositeness of a number. For a given integer *n*, choose some integer *a* with GCD (*a*, *n*) = 1 and compute $r \equiv a^{n-1} \pmod{n}$. If the modulo *n* computation give the results not equal to 1, *n* is composite. Otherwise, *n* probably prime, in other words, *n* can be prime or composite.

2.4 Algorithm of Fermat Test

Input: an integer $n \geq 3$.

Output: n is prime or n is composite

1. *Choose random integer a with $2 \leq a \leq n-1$ and GCD (a, n) = 1.*
   - *1.1 Compute $r \equiv a^{n-1} \pmod{n}$.*
   - *1.2 If $r \neq 1$, n is composite, otherwise n is prime number.*
2. *If GCD (a, n) $\neq$ 1, then n is composite.*

Here, when GCD $(a, n) \neq 1$, *n* is certainly composite because it is implies that *n* has another divisors beside 1 and itself, which is contradict with definition of prime number. If GCD (*a*, *n*) = 1, *n* can be composite or prime number.

2.5 Source Code of Fermat Test

By coding the Algorithm into *Mathematica* (6.0 version), here is the source code:

```
a=__;
n=__;
If [2≤a≤n-1,If [GCD [a,n]==1,
r =PowerMod [a,n-1,n];
If[r≠1,n "is composite",n "is
Prime"],n "is composite
"],"cannot be proceed, pick a
any integer 2≤a≤n-1"]
```

Once this is executed, if the input is a prime number then it will tells you that ***n is a prime***.

Otherwise it will gives you a message ***n is a composite***. Take notes, there are numbers which also identified as prime numbers even though they are not. These numbers are called pseudoprimes. This is due again to the Fermat's theorem. This source code can also identify Carmichael numbers (absolute pseudoprimes). Carmichael number is a pseudoprime for all bases *a*. From the output produced by this test, we have tabled list of primes for every base *a* which are less than 10,000. The build-in Mathematica command, "PrimeQ[*integer*]" is used to verify the primality of the test output and from here can be

identified the pseudoprimes, then the command, "PrimePi[10,000]", is used to compute percentage of pseudoprimes. The smaller the percentage is, the better the ability of the test is, as this indicates the accuracy of the test. To look for Carmichael numbers, just need to look out for common pseudoprimes for each base a. Here, the author restrict the choice of the base a from 2 until 20 only. For a complete computation of pseudoprimes and Carmichael numbers refer to (Gradini, 2009).

3. Fermat Pseudo-prime

Let n is a Fermat pseudo-primes (simply called pseudo-prime) if $a^{n-1} \equiv 1 \pmod{n}$ but n is a composite number. Generally, a composite number n such that $a^{n-1} \equiv 1 \pmod{n}$ is a pseudoprime to base a.

Fermat pseudo-prime exists since Fermat's Little Theorem occurs in the way, recall that the theorem says if n is prime number then $a^{n-1} \equiv 1 \pmod{n}$, is necessarily true that when $a^{n-1} \equiv 1 \pmod{n}$, n is a prime number.

Example 3.1

1. 341 is pseudo-prime to base 3.
   It has already known that 341 is composite since $341 = 11 \times 31$, but 341 passes Fermat test, since $3^{341-1} \equiv 1 \pmod{341}$.
2. 217 is pseudo-prime to base 5.
   $217 = 7 \times 31$, then 217 is composite, but $5^{217-1} \equiv 1 \pmod{217}$, then 217 passes Fermat test.

Table 3.1 List of pseudo-prime $< 10{,}000$ with $2 \leq a \leq 20$

a	Pseudo-prime ≤ 10 000	n(psp)
2	341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911	22
3	91, 121, 286, 671, 703, 949, 1105, 1541, 1729, 1891, 2465, 2665, 2701, 2821, 3281, 3367, 3751, 4961, 5551, 6601, 7381, 8401, 8911	23
4	15, 85, 91, 341, 435, 451, 561, 645, 703, 1105, 1247, 1271, 1387, 1581, 1695, 1729, 1891, 1905, 2047, 2071, 2465, 2701, 2821, 3133, 3277, 3367, 3683, 4033, 4369, 4371, 4681, 4795, 4859, 5461, 5551, 6601, 6643, 7957, 8321, 8481, 8695, 8911, 9061, 9131, 9211, 9605, 9919	47
5	124, 217, 561, 781, 1541, 1729, 1891, 2821, 4123, 5461, 5611, 5662, 5731, 6601, 7449, 7813, 8029, 8911, 9881	19
6	35, 185, 217, 301, 481, 1105, 1111, 1261, 1333, 1729, 2465, 2701, 2821, 3421, 3565, 3589, 3913, 4123, 4495, 5713, 6533, 6601, 8029, 8365, 8911, 9331, 9881	27
7	25, 325, 561, 703, 817, 1105, 1825, 2101, 2353, 2465, 3277, 4525, 4825, 6697, 8321	15
8	9, 21, 45, 63, 65, 105, 117, 133, 153, 231, 273, 341, 481, 511, 561, 585, 645, 651, 861, 949, 1001, 1105, 1281, 1365, 1387, 1417, 1541, 1649, 1661, 1729, 1785, 1909, 2047, 2169, 2465, 2501, 2701, 2821, 3145, 3171, 3201, 3277, 3605, 3641, 4005, 4033, 4097, 4369, 4371, 4641, 4681, 4921, 5461, 5565, 5963, 6305, 6533, 6601, 6951, 7107, 7161, 7957, 8321, 8481, 8911, 9265, 9709, 9773, 9881, 9945	70
9	28, 52, 91, 121, 205, 286, 364, 511, 532, 616, 671, 697, 703, 946, 949, 1036, 1105, 1288, 1387, 1541, 1729, 1891, 2465, 2501, 2665, 2701, 2806, 2821, 2926, 3052, 3281, 3367, 3751, 4376, 4636, 4961, 5356 ,5551, 6364, 6601, 6643,7081, 7381, 7913, 8401, 8695, 8744, 8866, 8911	49
10	33, 91, 99, 259, 451, 481, 561, 657, 703, 909, 1233, 1729, 2409, 2821, 2981, 3333, 3367, 4141, 4187, 4521, 5461, 6533, 6541, 6601, 7107, 7471, 7777, 8149, 8401, 8911	30
11	65, 70, 133, 190, 259, 305, 481, 645, 703, 793, 1105, 1330, 1729, 2047, 2257, 2465, 2821, 4577, 4921, 5041, 5185, 6601, 7869, 8113, 8170, 8695, 8911, 9730	28
12	65, 91, 133, 143, 145, 247, 377, 385, 703, 1045, 1099, 1105, 1649, 1729, 1885, 1891, 2041, 2233, 2465, 2701, 2821, 2983, 3367, 3553, 5005, 5365, 5551, 5785, 6061, 6305, 6601, 8911, 9073	33
13	21, 85, 105, 231, 244, 276, 357, 427, 561, 1099, 1785, 1891, 2465, 2806, 3605, 5028, 5149, 5185, 5565, 6601, 7107, 8841, 8911, 9577, 9637	25
14	15, 39, 65, 195, 481, 561, 781, 793, 841, 985, 1105, 1111, 1541, 1891, 2257, 2465, 2501, 2641, 2665, 2743, 3277,5185, 5713, 6501, 6533, 6541, 7107, 7171, 7449, 7543, 7585, 8321, 9073	32
15	341, 742, 946, 1477, 1541, 1687, 1729, 1891, 1921, 2821, 3133, 3277, 4187, 6541, 6601, 7471, 8701, 8911, 9073	19
16	51, 85, 91, 255, 341, 435, 451, 561, 595, 645,703, 1105, 1247 , 1261, 1271, 1285, 1387, 1581, 1687, 1695, 1729, 1891, 1905, 2047, 2071, 2091, 2431,	63

2701, 2821, 3133, 3277, 3367, 3655, 3683, 4033, 4369, 4371, 4681, 4859, 5083, 5151, 5461, 5551, 6601, 6643, 7471, 7735, 7957 , 8119, 8245, 8321, 8481, 8695, 8749, 8911, 9061, 9131, 9211, 9605, 9919		
, 145, 261, 781, 1111, 1228, 1305, 1729, 1885, 2149, 2821, 3991, 4005, 4187, 4912, 5365, 5662, 5833, 6601, 6697, 7171, 8481, 8911	25	2.03%
, 65, 85, 133, 221, 323, 325, 343, 425, 451, 637, 931, 1105, 1225, 1369, 1649, 1729, 1921, 2149, 2465, 2701, 2821, 2825, 2977, 3325, 4165, 4753, 5525, 5725, 5833, 5941, 6305, 6517, 6601, 7345, 8911, 9061	40	3.25%
, 153, 169, 343,561, 637, 889, 905, 906, 1035, 1105, 1629, 1661, 1849, 2353, 2465, 2701, 2821, 2955, 3201, 4033, 4681, 5461, 5466, 5713, 6541, 6601, 6697, 7957, 8145, 8281, 8401, 8869, 9211, 9997	38	3.09%
7, 133, 231, 399, 561, 671, 861, 889, 1281, 1653, 1729, 1891, 2059, 2501, 2761, 2821, 2947, 3059, 3201, 4047, 5271, 5461, 5473, 5713, 6601, 6817, 7999, 8421, 8911	32	2.60%

Table 3.1 gives the distribution of pseudo-prime $\leq 10{,}000$ at every base *a*, the number of pseudo-prime is denoted as *n(psp).* All of those pseudo-prime numbers get by comparing the solution (output) of Fermat test with the list of primality of positive integers $\leq 10{,}000$ as exact solution. The exact solution was get from built-in program in *Mathematica* (6.0 version). Then the output of Fermat test and Exact solution are used as input to perform the pseudo-prime by using a syntax in *Mathematica*(6.0 version), Complement[x_,y_].

Based on Table 2.2 number of prime number $\leq$10,000 is 1229. Then by dividing *n(psp)* by 1229, we can get the percentage of pseudo-prime at each base. In prime number $\leq 10{,}000$, $2 \leq a \leq 20$, base 8 produces the biggest number of pseudoprime, that reach 5.70 %, while the smallest number of pseudoprime (1.22%) produced by base 7. From the table above, it can be seen that pseudo-prime are rare in prime number, but it is not rare enough to be ignored.

3.1 Carmichael Number

A Carmichael numbers *n* is of composite number *n* with the property that for every base *a*, $a^{n-1} \equiv 1 \pmod{n}$. It follows that a Charmichael number *n* must be square free, with at least three prime factors, and that $p\text{-}1 \mid n\text{-}1$ for every *p* dividing *n* (Pinch, 2007).

There are 7 Carmichael number $\leq$ 10,000. Carmichael number does not appear at all base in Table 3.1, because by properties, a pseudo-prime is Carmichael number if satisfies:

1. Square-free
2. Has prime factor at least 3, and for every prime factor *p*, $p - 1 \mid n - 1$
3. Passes Fermat test at base *a* where GCD (*a*, *n*) = 1

For seeing the Carmichael numbers within Fermat Pseudoprimes, please refer to (Gradini, 2009)

4. Conclusion

Using Mathematica 6.0 for the primality tests, the author has managed to conduct technical tasks and perform the ability of the primality tests discussed earlier. These technical tasks were usually done using programming languages which take very long time to do the source code.

For example programming language C or C++ and other programming languages that requires deep understanding and time consuming. There are absolute pseudo-prime (Carmichael numbers) in Fermat test, but not on the other tests and Fermat has the large number of prime which is very far from the exact number.

DAFTAR KEPUSTAKAAN

Bektas,Attila.(2005). *Probabilistic Primality Test*. Master's Thesis. The Middle East Technical University.

Eynden,Charles Vanden.(2001). *Elementary number theory.2nd edn.* Illnois : McGraw-Hill

Gradini,Ega. 2009. *Primality Testing.* Project report of MSc in Teaching of Mathematics, Universiti Sains Malaysia.

Jones,Gareth A &Jones, Mary J.(1998).*Elementary number theory*.London:springer-Verlag

Kumanduri,Ramanujachary &Romero,cristina,(1998). Number Theory with computer Application.New Jersey : Prentice-Hall

McIntosh,Christina.(2007). finding Prime Numbers: Miller-Rabin and Beyond.Electronic Journal of Undergraduate Mathematics.[Online],2007(12).[Acessed 5th January 2009],Availabale from World Wide Web : www.scribd.com/doc/4904376/FINDING-PRIME-NUMBER -