The Bulletin of Society for Mathematical Services and Standards *Online: 2014-06-02*
ISSN: 2277-8020, Vol. 10, pp 26-30
doi:10.18052/www.scipress.com/BSMaSS.10.26

Existence of Poluet numbers in square form

D. Narasimha Murty[1] and Prof. Dr. K. Raja Rama Gandhi[2]

Research Scholar, Department of Mathematics, AMET University, Chennai[1]
Resource person in Math for Oxford University Press and Professor in Math at BITS-Vizag[2]
Email: rrmath28@gmail.com

Keywords: Fermat little theorem, poulet number

ABSTRACT. In this paper, we will introduce theorem, which will generate Fermat Pseudo primes in different base system. Also, by fixing base-2, we find first poulet number and we show the first square type poulet number by suitable example and theorem.

1. INTRODUCTION

We know that, Primes are playing vital role in Computer Science, especially in Cryptography (see [1] & [2]) algorithms to strengthen security systems. In this connection, we are studying on Fermat Pseudo primes [3] (special primes) to more strengthen the cryptography in elegant way. As we know that, these Fermat Pseudo primes are born from Fermat little theorem and there is no much difference in both, except the prime case.
Let us observe the definitions and generalizations of Fermat little theorem [4] and Fermat Pseudo primes.

Definition #1: If p is a prime number and a is any other natural number not divisible by p, then the number $a^{p-1}-1$ is divisible by p.
Or $a^{p-1} \equiv 1(\text{mod } p)$

Example #1: For p = 7 and a = 12, by cited above definition, we have;

$$a^{p-1} \equiv 1(\text{mod}\, p) \Rightarrow 12^{7-1} \equiv 1(\text{mod}7)$$

$$\Rightarrow 12^{6} \equiv 1(\text{mod}7)$$

$$\Rightarrow 7 \mid 12^{6}-1 \Rightarrow 7 \mid 2985983$$

$$\therefore 426569.$$

Let us observe another example:
Example #2: For p = 341 and a = 2, by cited above definition, we have;

$$a^{p-1} \equiv 1(\text{mod } p) \Rightarrow 2^{341`-1} \equiv 1(\text{mod } 341)$$

$$\Rightarrow 2^{340} \equiv 1(\text{mod } 341)$$

$$= 341 \mid 2^{340}-1 \bullet$$

Here p is not a prime, as 341 have prime factors. i.e., 11 and 31.
Thus, we can redefine Fermat Pseudo primes as follows:
If Fermat little theorem satisfies for non-prime p (say m), we call such m as Fermat Pseudo prime.

Definition #2: If m is a non-prime integer and a is any other natural number not divisible by m, then the number $a^{m-1}-1$ is divisible by m.
Or $a^{m-1} \equiv 1(\text{mod } m)$.
We believe that, there are many such Pseudo primes are existing, and these can be classified by base system. Interestingly we have taken base-2 in the example-2 above. There are many Pseudo primes exist in different base system. At this point of time, we are interested in 2-base or bsae-2 ie.,

a = 2. The reason for choosing base-2 is, the base-2 Pseudo primes are known as *Poulet numbers* [5] and we make some observations on base-2 Fermat Pseudo primes or Poulet numbers.
Thus, 341 is called as Fermat Pseudo prime as well as Poulet number. In the next section, we will discuss the generation of base-a Pseudo prime with theorem.

2. FERMAT PSEUDO PRIMES IN DIFFERENT BASE SYSTEM

This is the time to search number of availability of Fermat pseudo primes in different bases. Interestingly we came up with theorem, which generates infinitely many such primes. Let us state proposition and theorem.

Proposition 2.1: For any integer *a* and prime *p,* the result of $a^p + a$ is an even integer.
Proof: let us take *a* in two cases.
Case#1: If *a* is odd integer, then we have $a \equiv 1(\text{mod}2)$
Or $a^p \equiv 1(\text{mod } 2)$
$\Rightarrow a^p + a = 2(\text{mod}2) \Leftrightarrow a^p + a = 0(\text{mod}2)$
$\therefore a^p + a = 2n$, for some integer n.
Case #2: If a is even integer, then we have $a = 0(\text{mod}2)$
Or $a^p \equiv 0(\text{mod } 2)$
$\Rightarrow a^p + a = 0(\text{mod}2)$
$\therefore a^p + a = 2n$, for some integer n.

Theorem 2.2: For an odd prime *p* and not dividing $a^2 - 1$, with (a, p) =1; then $m = \dfrac{a^{2p} - 1}{a^2 - 1}$ is pseudo primes in base-a for a > 1.
Proof: let us list, what we have to prove exactly:
(i) *m* has to factors (not necessarily equal prime factors or square free)
(ii) *m* is odd integer
(iii) *m* satisfies Fermat little theorem or $a^{m-1} \equiv 1(\text{mod } m)$

We have $m = \dfrac{a^{2p} - 1}{a^2 - 1} = m(a^2 - 1) = a^{2p} - 1.$
Or $m \mid a^{2p} - 1$ (1)

Now $m = \dfrac{a^{2p} - 1}{a^2 - 1} = \left(\dfrac{a^p - 1}{a - 1}\right)\left(\dfrac{a^p + 1}{a + 1}\right)$ (*A*)

$$m = \frac{a^{2p} - 1}{a^2 - 1}$$

$$\Rightarrow m - 1 = \frac{a^{2p} - a^2}{a^2 - 1}$$

$$= a\left(\frac{a^{p-1} - 1}{a^2 - 1}\right)(a^p + a) \quad (2)$$

Here *m-1* is product of three integers and by preposition 2.1, m -1 is even integer
Or m is odd integer (*B*)

From (2), (a, p) =1 and $(p, a^p + a) = 1$, p should dived $\dfrac{a^{p-1} - 1}{a^2 - 1}$
Or m -1 = 2p (keeping $a^p + a$ is an even integer in mind)
Or $a^{m-1} = a^{2p} \Rightarrow a^{m-1} - 1 = a^{2p} - 1$
From (1), $a^{m-1} \equiv 1(\text{mod } m)$ (*C*)
(A), (B) and (C) respectively hold for (i) , (ii) and (iii) above.

Note: From the cited above theorem, one can generate many Fermat pseudo primes (not necessarily) in base-a.
Let us plug some choose *a* and *p* values in the above theorem:
Let us take *a = 2* and *p = 2*. Since *p* does not divide *a2 -1*, we can generate pseudo prime *m* by the cited above theorem.

$$\Rightarrow m = \frac{a^{2p}-1}{a^2-1} = \frac{2^4-1}{3} = 5$$

Here 5, is not pseudo prime as 5 does not have two equal or distinct prime factors.
Let us take *a = 2* and *p = 3*. Here *p* divides a^2 *-1*, we cannot generate pseudo prime *m* by the cited above theorem.
Let us take *a = 2* and *p = 5*. Here *p* does not divides a^2 *-1*, we can generate pseudo prime *m* by the cited above theorem.

$$\Rightarrow m = \frac{a^{2p}-1}{a^2-1} = \frac{2^{10}-1}{3} = \frac{1023}{3} = 341$$

Since we fixed base-2, one can call it is poulet number, instead of Fermat pseudo prime.
In fact, 341 is first poulet number.
Let us discuss the integer 121 is Fermat pseudo prime or poulet number.

$$2^{120}-1 = (2^{60}+1)(2^{60}-1)$$

$$= (2^{60}+1)(2^{30}+1)(2^{30}-1)$$

$$= (2^{60}+1)(2^{30}+1)(2^{15}+1)(2^{15}-1)$$

$$2^{15}-1 = 32767 \equiv 97(\mathrm{mod}121)$$

But $2^{15}+1 \equiv 99(\mathrm{mod}121)$

$$\Rightarrow (2^{60}+1)(2^{30}+1)(97)(99)(\mathrm{mod}121)$$

$$= (2^{60}+1)(44)(46)(\mathrm{mod}121) \equiv (90)(88)(\mathrm{mod}121)$$

$$\equiv 55(\mathrm{mod}121)$$

Therefore, 121 is not Fermat pseudo prime as well as poulet number.
But the following table says, there are some Fermat pseudo primes which are square numbers.
Let us observe the following Table #1.

Table #1 [6]

a	smallest p-p	*a*	smallest p-p	*a*	smallest p-p	*a*	smallest p-p
1	$4 = 2^2$	51	$65 = 5 \cdot 13$	101	$175 = 5^2 \cdot 7$	151	$175 = 5^2 \cdot 7$
2	$341 = 11 \cdot 31$	52	$85 = 5 \cdot 17$	102	$133 = 7 \cdot 19$	152	$153 = 3^2 \cdot 17$
3	$91 = 7 \cdot 13$	53	$65 = 5 \cdot 13$	103	$133 = 7 \cdot 19$	153	$209 = 11 \cdot 19$
4	$15 = 3 \cdot 5$	54	$55 = 5 \cdot 11$	104	$105 = 3 \cdot 5 \cdot 7$	154	$155 = 5 \cdot 31$
5	$124 = 2^2 \cdot 31$	55	$63 = 3^2 \cdot 7$	105	$451 = 11 \cdot 41$	155	$231 = 3 \cdot 7 \cdot 11$

6	$35 = 5 \cdot 7$	56	$57 = 3 \cdot 19$	106	$133 = 7 \cdot 19$	156	$217 = 7 \cdot 31$
7	$25 = 5^2$	57	$65 = 5 \cdot 13$	107	$133 = 7 \cdot 19$	157	$186 = 2 \cdot 3 \cdot 31$
8	$9 = 3^2$	58	$133 = 7 \cdot 19$	108	$341 = 11 \cdot 31$	158	$159 = 3 \cdot 53$
9	$28 = 2^2 \cdot 7$	59	$87 = 3 \cdot 29$	109	$117 = 3^2 \cdot 13$	159	$247 = 13 \cdot 19$
10	$33 = 3 \cdot 11$	60	$341 = 11 \cdot 31$	110	$111 = 3 \cdot 37$	160	$161 = 7 \cdot 23$
11	$15 = 3 \cdot 5$	61	$91 = 7 \cdot 13$	111	$190 = 2 \cdot 5 \cdot 19$	161	$190=2 \cdot 5 \cdot 19$

Now, the question is, can we find numbers like Fermat Pseudo primes (square numbers) in list of poulet numbers? If yes, what are those numbers? We have observed the proposition and we realized the existence of such square type poluet numbers.

$$\frac{2^{p-1}-1}{p}$$

Proposition 2.3: Find all primes *p* such that square. perfect is

Proof: Consider for time being;

$$\frac{2^{p-1}-1}{p} = m^2 \Rightarrow 2^{p-1} - 1 = pm^2$$

Let $p = 2k + 1$ for some $k \in N$.

Or $2k = p - 1$

$$\Rightarrow 2^{2p-1} = 2^{2k} - 1$$

$$\Rightarrow (2^k - 1)(2^k + 1) = pm^2 \quad (1)$$

Here $(2^k - 1, 2^k + 1) = 1$, since $(2^k - 1)$ and $(2^k + 1)$ are consecutive odd integers.

From (1), we may assume that; $2^k - 1 = px^2$ and $2^k + 1 = y^2$

Or $2^k - 1 = x^2$ and $2^k + 1 = py^2$

Case #1: $2^k - 1 = px^2$ and $2^k + 1 = y^2$

Take $2^k + 1 = y^2 \Rightarrow 2^k = y^2 - 1 \Leftrightarrow 2^k = (y-1)(y+1)$

i.e., $(y-1) = 2^n$ and $(y+1) = 2^m$ for some $m, n \in N \cup \{0\}$

The only possible *m* and *n* are 2 and 1 respectively.

Since $(y+1) = 2^m \Rightarrow y = 3.$

And from $2^k + 1 = y^2 \Rightarrow 2^k = 8$ for $y = 3.$

We get $k = 3.$

Clearly, *p* must be 7.

Similarly in other case, we get $p = 3.$

$$\frac{11^{p-1}-1}{p}$$

Proposition 2.4: Find all primes *p* such that is perfect square.

Proof: We are leaving the proof for readers.

The above cited preposition 2.3 gave me an idea to search poulet numbers in square form, and interestingly we got the good stuff!

Theorem 2.5: There exists at least one poulet number, which is in perfect square form.

Proof: We know that, poluet number *m* satisfies $2^{m-1} = 1(\text{mod } m)$.

We are finding some suitable *m,* such that $m = n^2$ for some $n \in N$.

$\Rightarrow 2^{m-1} = 1(\text{mod} m) \Rightarrow 2^{n^2-1} = 1(\text{mod} n^2)$

However, $2^{(n-1)(n+1)} - 1 = (2^{n-1} - 1)(1 + 2^{n-1} + 2^{2(n-1)} + 2^{3(n-1)} + ... + 2^{n(n-1)})$ (1)

Clearly, n^2 | (1) (in some cases)

The following counter examples will describe the existence of square form poulet numbers.

Example 2.6: Take n = 1 then, m = 1

$\Rightarrow 2^{m-1} = 1(\text{mod } m) \Rightarrow 2^0 = 1(\text{mod } 1).$

But 1 is not poulet, as '1' does not have prime factors.

Example 2.7: Take m = 12327121, then n = $(3511)^2$

Clearly the value of *m* satisfies $2^{m-1} = 1(\text{mod } m)$. Since 3511^2 is Wieferich prime [7]

But $12327121=(3511)^2$ and 3511 is not prime, as 3511= (47)(113)

Example 2.8: Take m = 1194649, then n = $(1093)^2$

Clearly the value of *m* satisfies $2^{m-1} = 1(\text{mod } m)$. Since 1093^2 is Wieferich prime [7]

Great! 1093 itself a prime and we achieved.

CONCLUSIONS

In this paper, we discussed the generation of pseudo primes and concluded the first poulet number by inspection. Also we found the first square type polut number in base -2 system. We believe that it is the only first number , since 1093 and 3511 are only know Wieferich primes so far.

ACKNOWLEDGEMENT

The first author is thankful to his parents and second author for their encouragement and support during the development of this paper.

REFERENCES

[1] Cryptography Engineering: Design Principles and Practical Applications by Niels Ferguson, Bruce Schneier and Tadayoshi Kohn, Wiley Publishing Inc, Canada, 2010.

[2] A Course in Number Theory and Cryptography by NEAL Koblitz, 2nd edition, Springer-Verlag New York, Inc 1994

[3] 17 Lectures on Fermat Numbers: From Number Theory to Geometry by Michal Florian Luca, Lawrence Somer, CMS Books in Mathematics, Springer, 2002.

[4] Elementary Number Theory with Applications by Thomas Koshy, 2nd edition, Elsevier, USA 2007.

[5] http://people.csail.mit.edu/kuat/courses/dirichlet.pdf

[6] http://en.wikipedia.org/wiki/Fermat_pseudoprime

[7] http://en.wikipedia.org/wiki/Wieferich_prime