International Journal of Engineering, Science and Mathematics
Vol. 6 Issue 8, December 2017 (Special Issue)
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Exquisite Explanation for the Recognized Conjecture on Fermat Pseudoprimes in Square Form

Narasimha murty Dusi*

Abstract

In this paper we will solve conjecture posed by M.Coman on primes by giving suitable example. We will bring a generalized theorem for square primes, which will deal with the generalization of Fermat Pseudoprime, which gives infinitely many pseudoprimes for different base system.

Keywords:

Fermat little theorem;
Fermat pseudoprime;
Weifrich primes;

Author correspondence:

[1]Assistant Professor, Department of Mathematics,
Baba Institute of Technology and Sciences, Andhrapradesh, INDIA

1. Introduction

We know that prime numbers are playing a critical role in computer science, particularly in to strengthen crypto system[1]&[2]. In connection to this we are dealing with Fermat pseudoprimes[3], after that poulet number and Carmichael numbers are developed. Basically Fermat little theorem[4] is the base for Fermat pseudoprime.

2. Materials and Methods

Let us observe the Fermat little theorem,

Deifinition#1: If p is any prime number and GCD of (a,p) is 1, then

$$a^{p-1} \equiv 1(\bmod p) \text{ or } \frac{a^{p-1}-1}{p}$$

Example#1: $p = 3, a = 2$ also $(3,2) = 1$

$$\Rightarrow 2^3 \equiv 1(\text{mod}3) \Rightarrow 3 | 2^{3-1} - 1 = \frac{3}{3} = 1$$

Example#2: $p = 7, a = 3$ also $(7,3) = 1$

$$\Rightarrow 3^{7-1} \equiv 1(\text{mod}7)$$

[*] Doctorate Program, Linguistics Program Studies, Udayana University Denpasar, Bali-Indonesia (9 pt)

$$=\frac{3^6-1}{7}=\frac{729-1}{7}=104$$

Similarly

Example#3: $p=341, a=2$ also $(341,2)=1$

$$\Rightarrow 2^{341-1}\equiv 1(\mathrm{mod}\,341)$$

$$\Rightarrow \frac{2^{340}-1}{341}=\frac{2239744742177804210557442280568444278121645497234649534899989100963791871180160945380877493271607115775}{341}$$

$$\Rightarrow 65681663993483994444499773623708043346675821033274179909090538947107894050381703652143335757394742275$$

Here 341 is not a prime number, it can be factorized into prime factors

Now we can modify the Fermat little as follows

Definition#2: If m is a composite number and GCD of m and a is 1 i.e (m,a)=1 then the number m divides $a^{m-1}-1$

Or $a^{m-1}\equiv 1(\mathrm{mod}\, m)$

Means 'm'is not necessarily a prime number, there is no much difference except in prime case between Fermat pseudoprime and Fermat little.

Example#4: $p=65, a=51$ also $\gcd(65,51)=1$

Here $65=5\times 31$ are prime factors

$$\Rightarrow 5\,|\,51^{51-1}-1=\frac{6765200}{5}=1353040$$

and $13|51^{51-1}-1=\frac{309629344375621415600}{13}=23817641875047801200$

Example#5: $\mathrm{n}=101, \mathrm{p}=175$

Here 175 $=5\ \mathrm{X}\ 5\ \mathrm{X}\ 7$ are prime factors

$$\Rightarrow \frac{101^{7\text{-}1}\text{-}1}{7}=\frac{1061520150600}{7}=151645735800$$

From this we can understand that there exists infinitely many pseudoprimes, but these are classified by different base system.

Conjecture:

The square of any odd prime can be obtained from the numbers of the form 360*k + 72 in the following way: let d1, d2, ..., dn be the (not distinct) prime factors of the number 360*k + 72; than for any square of a prime p^2 there exist k such that (d1 - 1)*(d2 - 1)*...*(dn - 1) + 1 = p^2.

Generalizes theorem for Fermat Pseudoprimes for different base system to generate infinitely many pseusopirmes:

Theorem#1: For an odd prime $'p'$ does not divides a, that is GCD of (a,p)=1 and p does not divides a^2-1 then $m(a^2-1)=a^{2p}-1$.

Proof:

By Fermat little theorem we have $a^{2p}\equiv a^2(\mathrm{mod}\, p)$

i.e. $\dfrac{a^{2p}-a^2}{p}\rightarrow(1)$

by the hypothesis we

have $m(a^2-1)=a^{2p}-1$

i.e. we can say that $\dfrac{a^{2p}-1}{m}$ -----------------(2)

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

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

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

$$\Rightarrow \frac{m-1}{p}\left[\because \frac{a^{2p}-a^2}{p}\ from(1)\right]$$

Also here $m-1$ is the sum of even numbers that all are of same party

Here $m-1=\dfrac{a^{2p}-a^2}{a^2-1}$ is the product of two numbers $\left(\dfrac{a^p-a}{a-1}\right)\left(\dfrac{a^p+a}{a+1}\right)$--------------(3)

In the above product $\left(\dfrac{a^p+a}{a+1}\right)$ is even number since a^p+a is even number

If a is odd integer $a\equiv 1(\mathrm{mod}\,2)\Rightarrow a^p\equiv 1^p(\mathrm{mod})\equiv 1(\mathrm{mod})\Rightarrow a^p+a\equiv 2(\mathrm{mod}\,2)\equiv 0(\mathrm{mod}\,2)$

If a is even integer $a\equiv 0(\mathrm{mod}\,2)\Rightarrow a^p\equiv 0(\mathrm{mod})\Rightarrow a^p+a\equiv 0(\mathrm{mod}\,2)$

Which implies that $m-1$ is even number i.e m is odd number----------------------(4)

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

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

From (2) implies $\dfrac{a^{2p}-1}{m}$ which clears that $a^{m-1}-1$ is divisible by m

Therefore m is a Fermat pseudo prime.

By the above theorem we can generate as many as pseudoprimes in different bases.

In particular base-2 pseudoprimes are called poulet numbers.Fixing base-2 and plug the values for $p=2,3,5...$ we can generate different Fermat psuedoprimes in different bases particularly base-2 (poulet numbers).

We cannot take $p=2$ since GCD(2,2) is 2 which contradicts to our hypothesis of above theorem

We cannot take $p=3$ since p divides a^2-1 which contradicts to our hypothesis of above theorem.

Let us take $p=5$ and $a=2$ then $m=\dfrac{a^{2p}-1}{a^2-1}=\dfrac{2^{10}-1}{4-1}=\dfrac{1024-1}{3}=341$

Here the obtained number 341 is the base-2 Fermat pseudoprime, also which is the first base-2 Fermat pseudoprime(Poulet number).

But we can observed from the following table some pseudoprimes in square form

a	smallest p-p	*a*	smallest p-p	*a*	smallest p-p	*a*	smallest p-p
1	4 = 2²	51	65 = 5 · 13	101	175 = 5² · 7	151	175 = 5² · 7
2	341 = 11 · 31	52	85 = 5 · 17	102	133 = 7 · 19	152	153 = 3² · 17
3	91 = 7 · 13	53	65 = 5 · 13	103	133 = 7 · 19	153	209 = 11 · 19
4	15 = 3 · 5	54	55 = 5 · 11	104	105 = 3 · 5 · 7	154	155 = 5 · 31
5	124 = 2² · 31	55	63 = 3² · 7	105	451 = 11 · 41	155	231 = 3 · 7 · 11
6	35 = 5 · 7	56	57 = 3 · 19	106	133 = 7 · 19	156	217 = 7 · 31
7	25 = 5²	57	65 = 5 · 13	107	133 = 7 · 19	157	186 = 2 · 3 · 31
8	9 = 3²	58	133 = 7 · 19	108	341 = 11 · 31	158	159 = 3 · 53
9	28 = 2² · 7	59	87 = 3 · 29	109	117 = 3² · 13	159	247 = 13 · 19
10	33 = 3 · 11	60	341 = 11 · 31	110	111 = 3 · 37	160	161 = 7 · 23
11	15 = 3 · 5	61	91 = 7 · 13	111	190 = 2 · 5 · 19	161	190 = 2 · 5 · 19
12	65 = 5 · 13	62	63 = 3² · 7	112	121 = 11²	162	481 = 13 · 37
13	21 = 3 · 7	63	341 = 11 · 31	113	133 = 7 · 19	163	186 = 2 · 3 · 31
14	15 = 3 · 5	64	65 = 5 · 13	114	115 = 5 · 23	164	165 = 3 · 5 · 11

15	$341 = 11 \cdot 31$	65	$112 = 2^4 \cdot 7$	115	$133 = 7 \cdot 19$	165	$172 = 2^2 \cdot 43$
16	$51 = 3 \cdot 17$	66	$91 = 7 \cdot 13$	116	$117 = 3^2 \cdot 13$	166	$301 = 7 \cdot 43$
17	$45 = 3^2 \cdot 5$	67	$85 = 5 \cdot 17$	117	$145 = 5 \cdot 29$	167	$231 = 3 \cdot 7 \cdot 11$
18	$25 = 5^2$	68	$69 = 3 \cdot 23$	118	$119 = 7 \cdot 17$	168	$169 = 13^2$
19	$45 = 3^2 \cdot 5$	69	$85 = 5 \cdot 17$	119	$177 = 3 \cdot 59$	169	$231 = 3 \cdot 7 \cdot 11$
20	$21 = 3 \cdot 7$	70	$169 = 13^2$	120	$121 = 11^2$	170	$171 = 3^2 \cdot 19$
21	$55 = 5 \cdot 11$	71	$105 = 3 \cdot 5 \cdot 7$	121	$133 = 7 \cdot 19$	171	$215 = 5 \cdot 43$
22	$69 = 3 \cdot 23$	72	$85 = 5 \cdot 17$	122	$123 = 3 \cdot 41$	172	$247 = 13 \cdot 19$
23	$33 = 3 \cdot 11$	73	$111 = 3 \cdot 37$	123	$217 = 7 \cdot 31$	173	$205 = 5 \cdot 41$
24	$25 = 5^2$	74	$75 = 3 \cdot 5^2$	124	$125 = 5^3$	174	$175 = 5^2 \cdot 7$
25	$28 = 2^2 \cdot 7$	75	$91 = 7 \cdot 13$	125	$133 = 7 \cdot 19$	175	$319 = 11 \cdot 19$
26	$27 = 3^3$	76	$77 = 7 \cdot 11$	126	$247 = 13 \cdot 19$	176	$177 = 3 \cdot 59$
27	$65 = 5 \cdot 13$	77	$247 = 13 \cdot 19$	127	$153 = 3^2 \cdot 17$	177	$196 = 2^2 \cdot 7^2$
28	$45 = 3^2 \cdot 5$	78	$341 = 11 \cdot 31$	128	$129 = 3 \cdot 43$	178	$247 = 13 \cdot 19$
29	$35 = 5 \cdot 7$	79	$91 = 7 \cdot 13$	129	$217 = 7 \cdot 31$	179	$185 = 5 \cdot 37$
30	$49 = 7^2$	80	$81 = 3^4$	130	$217 = 7 \cdot 31$	180	$217 = 7 \cdot 31$
31	$49 = 7^2$	81	$85 = 5 \cdot 17$	131	$143 = 11 \cdot 13$	181	$195 = 3 \cdot 5 \cdot 13$
32	$33 = 3 \cdot 11$	82	$91 = 7 \cdot 13$	132	$133 = 7 \cdot 19$	182	$183 = 3 \cdot 61$
33	$85 = 5 \cdot 17$	83	$105 = 3 \cdot 5 \cdot 7$	133	$145 = 5 \cdot 29$	183	$221 = 13 \cdot 17$
34	$35 = 5 \cdot 7$	84	$85 = 5 \cdot 17$	134	$135 = 3^3 \cdot 5$	184	$185 = 5 \cdot 37$
35	$51 = 3 \cdot 17$	85	$129 = 3 \cdot 43$	135	$221 = 13 \cdot 17$	185	$217 = 7 \cdot 31$
36	$91 = 7 \cdot 13$	86	$87 = 3 \cdot 29$	136	$265 = 5 \cdot 53$	186	$187 = 11 \cdot 17$
37	$45 = 3^2 \cdot 5$	87	$91 = 7 \cdot 13$	137	$148 = 2^2 \cdot 37$	187	$217 = 7 \cdot 31$
38	$39 = 3 \cdot 13$	88	$91 = 7 \cdot 13$	138	$259 = 7 \cdot 37$	188	$189 = 3^3 \cdot 7$
39	$95 = 5 \cdot 19$	89	$99 = 3^2 \cdot 11$	139	$161 = 7 \cdot 23$	189	$235 = 5 \cdot 47$
40	$91 = 7 \cdot 13$	90	$91 = 7 \cdot 13$	140	$141 = 3 \cdot 47$	190	$231 = 3 \cdot 7 \cdot 11$
41	$105 = 3 \cdot 5 \cdot 7$	91	$115 = 5 \cdot 23$	141	$355 = 5 \cdot 71$	191	$217 = 7 \cdot 31$
42	$205 = 5 \cdot 41$	92	$93 = 3 \cdot 31$	142	$143 = 11 \cdot 13$	192	$217 = 7 \cdot 31$
43	$77 = 7 \cdot 11$	93	$301 = 7 \cdot 43$	143	$213 = 3 \cdot 71$	193	$276 = 2^2 \cdot 3 \cdot 23$
44	$45 = 3^2 \cdot 5$	94	$95 = 5 \cdot 19$	144	$145 = 5 \cdot 29$	194	$195 = 3 \cdot 5 \cdot 13$
45	$76 = 2^2 \cdot 19$	95	$141 = 3 \cdot 47$	145	$153 = 3^2 \cdot 17$	195	$259 = 7 \cdot 37$

46	$133 = 7 \cdot 19$	96	$133 = 7 \cdot 19$	146	$147 = 3 \cdot 7^2$	196	$205 = 5 \cdot 41$
47	$65 = 5 \cdot 13$	97	$105 = 3 \cdot 5 \cdot 7$	147	$169 = 13^2$	197	$231 = 3 \cdot 7 \cdot 11$
48	$49 = 7^2$	98	$99 = 3^2 \cdot 11$	148	$231 = 3 \cdot 7 \cdot 11$	198	$247 = 13 \cdot 19$
49	$66 = 2 \cdot 3 \cdot 11$	99	$145 = 5 \cdot 29$	149	$175 = 5^2 \cdot 7$	199	$225 = 3^2 \cdot 5^2$
50	$51 = 3 \cdot 17$	100	$153 = 3^2 \cdot 17$	150	$169 = 13^2$	200	$201 = 3 \cdot 67$

Table-1[6]

The above table will help us to find some square type pseudoprimes, with the help of them we can find the square type prime numbers. And also we can check all the primes are following the conjecture which is posed by M.Coman.

Proposition#1: Find all primes t such that $\dfrac{2^{t-1}-1}{t}$ is a perfect square

Proof:

Let us suppose that $\dfrac{2^{t-1}-1}{t}=u^2$

$2^{t-1}-1=u^2t$ ----- (1)

for $k \in N$ let us take $t=2k+1 \Rightarrow t-1=2k$

$2^{t-1}=2^{2k}$

$2^{t-1}-1=2^{2k}-1$

$\Rightarrow 2^{2k}-1=u^2t$ Then $(2^k+1)(2^k-1)=u^2t$, here $GCD(2^k+1)(2^k-1)=1$

From (1) let us assume that $2^k-1=px^2$ and $2^k+1=y^2$ ---- (2)

Or $2^k-1=x^2$ and $2^k+1=py^2$ ---- (3)

From (2) take $2^k=y^2-1 \Leftrightarrow (y-1)(y+1)=2^k$

$i.e.(y-1)=2^n$ and $(y+1)=2^m$ for some $m,n \in N \cup \{0\}$------(4)

The possible m and n are 2 and 1 respectively.

Since $y+1=2^m \Rightarrow y=2^2-1=3$ also $y-1=2^n \Rightarrow y=2^1-1=3$

Therefore $y=3$

From assumption $2^k+1=y^2$ which implies that $2^k+1=3^2 \Rightarrow k=3$

For $y=3\,,k=3$

clearly t must be prime , $t(prime)=7$

Result: This clears that $\dfrac{2^{7-1}-1}{7}=\dfrac{2^6-1}{7}=\dfrac{64-1}{7}=\dfrac{63}{7}=9(Perfect\ square)$

Now by cited above theorem we can get prime number in square form. The above preposition gives an idea to search for applicability of the above cited conjecture for all the square type prime numbers, fortunately on searching us successfully got a base-2 pseudoprimes in square form. By using that result we got scope to give a counter example to our conjecture which was posed by M Coman.

Theorem#2: There exists at least one base-2 Fermat pseudoprime in perfect square form[9]

Proof: We have from the definition $2^{p^2-1} \equiv 1(\bmod p^2)$

$$\Rightarrow \frac{2^{p^2-1}-1}{p^2} = \frac{2^{(p-1)(p+1)}-1}{p^2}$$ clearly p^2 divides the numerator in some cases.

The below example will clarify the above.

Example#6: Let us Take $p = 1093$ and $m = p^2 = 1194649$

Clearly m satisfies our definition, By the definition $2^{m-1} \equiv 1(\bmod m)$

$$2^{1194649-1} \equiv 1(\bmod 1194649)$$

$$\Rightarrow \frac{2^{1194648}}{1194649}$$

Since 1093 is one of the a Wiefrich prime, and other Wiefrich prime is 3511

We achieved and also 1093,3511 both are prime numbers itself.

Elegant solution for conjecture:

Let $d_1, d_2, d_3, \ldots d_n$ be the consecutive prime factors of a number $360*k+72$, then for any square prime p^2 then, $\exists k$ such that $(d_1-1)(d_2-1)\ldots(d_n-1)+1 = p^2$ [8]

Example#7: let us take the below 13 prime numbers 3,5,7,11…are obtained for k=1,11,4,6… respectively.

Let us take p=3 and k=1

$$360*1+72 = 432 = 2^4*3^3 = 1^4*2^3+1 = 9$$

Let us take p=5 and k=11

$$360*11+72 = 4032 = 2^6*3^2*7 = 1^6*2^2*6+1 = 25$$

Let us take p=7 and k=4

$$360*4+72 = 1512 = 2^3*3^3*7 = 1^3*2^3*6+1 = 49$$

Let us take p=11 and k=6

$$360*6+72 = 2232 = 2^3*3^2*31 = 1^3*2^2*30+1 = 121$$

But if we take the numbers 1093,3511 both are prime numbers and wiefrich primes so called,

Let us take p=1039 and k=18413

$$360*18413+72 = 3^3*4^1*8^1*14^1*548 = 2^3*3^1*7^1*13^1*547+1 = 1194649$$

but let us take p=3511 we cannot get in the above form

Test: $p = 3511,\ p^2 = 12327121$

$$= 12327120+1 = 2^4*3^3*5^1*577+1$$

The required form is $360*k+72 = 3^4*4^3*6^1*578 = 17978112$

$$\Rightarrow k = 49939.4$$

Conclusion :

With above counter example all the prime numbers in square form we cannot write in the form of $360*k+72=(d_1-1)(d_2-1)...(d_n-1)+1=p^2$ i.e. we cannot get a suitable k to write in the above form.

[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 Krizek, 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

[8]https://www.researchgate.net/publication/321003797 November 2017

[9] Existence of poulet numbers in square form by Bulletin of Society for Mathematical Services & Standards,Vol. 3 No. 2 (2014), pp. 46-5 May 2015