Bulletin of Mathematical Sciences and Applications *Online: 2014-05-01*
ISSN: 2278-9634, Vol. 8, pp 62-65
doi:10.18052/www.scipress.com/BMSA.8.62

Elegant solutions to Famous conjectures on Fermat Pseudoprimes -II

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

[1]Resource person in Math for Oxford University Press and Professor in Math at BITS-Vizag
[2]Research Scholar, Department of Mathematics, AMET University, Chennai

Email: rrmath28@gmail.com

Keywords: Fermat little theorem, Dirichlet thoerem

Abstract In this paper, we will solve two conjectures posed by *M. coman* on Fermat Pseudoprimes (base-2) or Poulet numbers by producing elegant proofs.

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 Pseudoprimes [3] (special primes) to more strengthen the cryptography in elegant way. As we know that, these Fermat Pseudoprimes 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 Pseudoprimes.

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.

$$\text{Or } a^{p-1} \equiv 1(\text{mod } p)$$

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

$$\begin{gathered} a^{p-1} \equiv 1(\text{mod}\, p) \Rightarrow 12^{7-1} \equiv 1(\text{mod}7) \\ \Rightarrow 12^6 \equiv 1(\text{mod}7) \\ \Rightarrow 7 \mid 12^6 - 1 \Rightarrow 7 \mid 2985983 \\ \therefore 426569. \end{gathered}$$

Let us observe another example:

Example #2: For p = 341 and a = 2, by cited above definition, we have;

$$\begin{gathered} a^{p-1} \equiv 1(\text{mod } p) \Rightarrow 2^{341`-1} \equiv 1(\text{mod } 341) \\ \Rightarrow 2^{340} \equiv 1(\text{mod } 341) \\ = 341 \mid 2^{340} - 1 \bullet \end{gathered}$$

Here p is not a prime, as 341 have prime factors. i.e., 11 and 31. Thus, we can redefine Fermat Pseudoprimes as follows:
If Fermat little theorem satisfies for non-prime p (say m), we call such m as Fermat Pseudoprime.
Definition #2: If m is a non-prime number and a is any other natural number not divisible by m, then the number $a^{m-1}-1$ is divisible by m.

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

We believe that, there are many such Pseudoprimes are existing, and these can be classified by base system. Interestingly we have taken base-2 in the example-2 above. There are many Pseudoprimes are existing 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 Pseudoprimes are known as *Poulet numbers*

[5] and we found two interesting conjectures on base-2 Fermat Psedoprimes or Poulet numbers. Thus, 341 is called as Fermat Pseudoprime as well as Poulet number. In the last section, we will discuss the generation of base-a Pseudoprime with theorem.
Let us address the conjectures in the next section.

Conjectures

The following conjectures are first stated by *M. Coman* without leaving proofs or generalizations. The first two conjectures of his collected papers are:

Conjecture #1: For any prime p, $p \geq 7$, there exist an infinity of primes q, $q > p$, such that the number $r=\frac{q-1}{p-1}$ is a natural number. In other words, for any such prime p there exist an infinity of natural numbers r such that $q = rp - r + 1$ is prime.

Conjecture #2: For any 2-Poulet number $P = d_1 d_2$, where $d_1 < d_2$, the following statement is true: the number $r=\frac{d_2-1}{d_1-1}$ is a rational number.
Let us introduce theorem, before prove/disprove the cited above conjectures.

Theorem 1: For an odd prime p and not dividing a^2-1, then $m=\frac{a^{2p}-1}{a^2-1}$ is pseudoprimes in base-a.

Proof: We know that, $a^p \equiv a(\text{mod } p) \Rightarrow a^{2p} \equiv a^2 (\text{mod}\, p)$ *ie.*, $p \mid a^{2p} - a^2$
But our hypothesis says that, p does not divides a^2-1.

We have;
$$m = \frac{a^{2p}-1}{a^2-1} \Rightarrow m-1 = \frac{a^{2p}-1}{a^2-1} - 1 = \frac{a^{2p}-a^2}{a^2-1}$$
$$\Rightarrow m-1 = \frac{a^{2p}-a^2}{a^2-1}.$$

$\Rightarrow p \mid m-1.$
In fact, looking closer at:
$$\sum_{i=1}^{p-1} a^{2(p-i)} = a^{2(p-1)} + a^{2(p-2)} + \ldots + a^2 \equiv m-1(\text{mod } p),$$
Also we have that; *m-1* is the sum of an even number of terms that all have the same parity. i.e., $2 \mid (m-1) \Rightarrow 2p \mid (m-1)$.
Then we have that, $(a^{2p}-1) \mid (a^{m-1}-1)$, and $a^{2p}-1 = m(a^2-1)$, which is multiple of m.
Thus, $a^{2p}-1 \equiv 0(\text{mod } m) \Rightarrow a^{m-1} \equiv 1(\text{mod } m)$ •

Note: From the cited above theorem, one can generate many Fermat pseudoprimes (not necessarily) in base-a.

Let us take $a = 2$ and $p = 2$. Since p does not divide $a^2 - 1$, we can generate pseudoprime 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 pseudoprime as 5 do not have prime factors. However, this will satisfy Fermat little theorem, as 5 itself a prime.
Let us take $a = 2$ and $p = 3$. Here p divides $a^2 - 1$, we cannot generate pseudoprime 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 pseudoprime m by the cited above theorem.

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

Therefore, we can realize that 341 is the first poulet number. **...(*)**
Also, we realize that **Conjecture #2** is wrong by the following illustration.

Let $d_1 = 17$ and $d_2 = 19$.

Now $r = \frac{d_2 - 1}{d_1 - 1} = \frac{18}{16} = \frac{9}{8}$

As per the conjecture r is rational.

Here $P = d_1 d_2 = 323$. This is not Poulet number.

In fact 341 is first poulet number by **(*).**

The **conjecture #1** is meaningful as $a_N = (p-1)r + 1$ contains infinitely many primes q by Dirichlet's theorem on arithmetic progressions [5]. Note that here $a_N = q$, and a_N is arithmetic progression.

New observation

Let us take two different Poulet numbers which have a common prime factor
i.e.

$$p_1 = 341 = 11 \times 31 \qquad p_2 = 4681 = 31 \times 151$$

Here 31 is common prime factor

Let us define the following recurrence formula

$$p_n = p_{n-2} + (p_{n-2} - 1, p_{n-1} - 1) \quad \ldots.(*)$$

Ex: First case:

$$(p_1, p_2) \equiv (341, 4681)$$

$$p_3 = p_1 + (p_1 - 1, p_2 - 1) \text{ from } (*)$$

$$= 341 + (340, 4680)$$

$$= 341 + 20$$

$$p_4 = p_2 + (p_2 - 1, p_3 - 1)$$
$$= 4681 + (4680, 360) = 5041$$

Like this we can find $p_5, p_6 \ldots$
Interestingly, we can observe that the values of;
$p_{14} = p_{15}$ and $p_{16} = p_{17}$ and so on…
But if we take, second case:

$p_1 = 1387$ and $p_1 = 2701$
By using the (*)
We can find p_3, p_4, p_5 and so on
Again here we see; $p_6 = p_{7,} p_8 = p_{9,} p_{10} = p_{11}$ and so on
Question:
Why does the (*) making $p_{14} = p_{15}$, $p_{16} = p_{17}$ and so on, as in the first case for fixed p_1 and p_2 Poulet numbers, as well as in the second case for $p_6 = p_{7,} p_8 = p_9$ and so on?
The above cited question is left for readers or will be answered in our next forthcoming paper(s).

Remark: we will address the other conjectures in our forthcoming paper, titled: Elegant solutions to Famous conjectures on Fermat Pseudoprimes –III and so on.

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 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