A Research on Fermat Little Theorem and Its Euler's Generalization: Selected Proofs

Sikander*

Assistant Professor of Mathematics, A.I.J.H.M. College Rohtak, Haryana, India

Abstractt – In this examination , we spread Fermat Little Theorem, Euler's generalization of this theorem, and. Fermat's Little Theorem, and Euler's theorem are two of the most significant theorems of present day number theory. Since it is so crucial, we set aside the effort to give two proofs of Fermat's theorem: (I) the acceptance based proof, and (ii) the change based proof. The second of these sums up to give a proof of Euler's theorem. There is a third proof utilizing bunch theory, however we center around the two increasingly rudimentary proofs. We present a few ways to deal with a conceivable "basic" proof of Fermat's Little Theorem (FLT), which expresses that for all n more prominent than 2, there don't exist x, y, z to such an extent that xn + yn = zn, where x, y, z, n, are certain whole numbers.

---------------------------------x---------------------------------

INTRODUCTION

Fermat's 'little' theorem is one of the gems of Number Theory, and to stamp the 400"1 commemoration of Fermat's introduction to the world, I offer this discussion. My discussion isn't proposed as a prologue to Number Theory, nor in fact even as a prologue to Maple, in spite of the fact that in the two cases it could fill in accordingly. Undoubtedly in the time accessible (somewhere in the range of 30 minutes) me will be able to cover just a little determination of the points recorded beneath. Any individual who is intrigued may get to the this Maple .mws record at my site, and furthermore a html content transformation (which might be perused by any individual who has an internet browser, and does not require having Maple); they are in the Public and Other Lectures area of the Maple segment of my website.

Then again his little theorem - which was generally simple to demonstrate (however what number of could make a proof stomach muscle initio?) - has a tremendous scope of numerical results, and one noteworthy practical application.

In this investigation we consider a portion of the early proofs of Fermat's Little Theorem. Our principle reference is History of the Theory of Numbers, Volume 1 by L.E. Dickson. Since a large number of the first sources to the proofs of these theorems are dark, we more often than not allude the peruser to Dickson. The grouping of the proofs shows up sequentially, so as to show how the proofs advanced all through the seventeenth twentieth hundreds of years.

One of our principle objectives is to take crude, inadequate proofs laid out in Dickson and fill in the missing subtleties. We do, in any case, attempt to hold the first kind of the proofs as for documentation and phrasing. Another objective is to underscore the extraordinary assortment of strategies that were utilized to demonstrate the two theorems and their generalizations.

THE USE OF 'LITTLE', THE THEOREM ITSELF, AND HOW IT ORIGINATED

The - little' of the theorem: When did this theorem begin to be called 'Fermat's little theorem? Who (in English) first called it so?

As a matter of fact not every person calls it so. In Vol I [1919] of Dickson's monumen¬tal three volume [.History of the] Theory of Numbers there is a whole part dedicated to 'Fermat's and Wilson's Theorems.' Hardy and Wright, Davenport, Nagell, ... , basically use 'Fermat's theorem.' And Sierpinski calls it 'Straightforward The¬orem of Fermat' in his 1964 .4 Selection of issues in the Theory of Numbers.

Obviously everybody realizes what 'Wilson's theorem' is - since there is just a single such theorem (at the same time, presumably, somebody will compose and let me know of another!) - yet 'Fermat'8 theorem'? Well there are a few petitioners: the lovely result - to name however one - that each prime p. with p= 1 (mod 4), is representable by p=a-+ t? for a few (remarkable; disregarding, obviously, change of signs, and inter¬change) whole numbers an and b, could well profess to be 'Fermat's theorem.'

The theorem itself : According to Dickson (and others: see Bibliography) Fermat previously declared his theorem in a letter to Mersenne, June (?), 1640.

Fermat's 'little' theorem. Give p a chance to be prime, and a be any number with a 0 (mod p), at that point In non-coinciding language: let p be any prime, and a be any whole number not detachable by p. at that point leaves leftover portion 1 on division by p.

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

A small hand performed illustration. Let p = 7 and a = 2, then $a^{(p-1)} = 2^6 \; = 64 = 7 * 9 + 1.$

Maple examples (the meaning of each command should be clear).

- restart;
- p[l] := nextprime(120);
- p, := 127
- a[l] := 2;
- ai := 2
- 57 mod 5; # the remainder 57 leaves on division by 5
- 2
- a[l]"(p[l] - 1);
- 85070591730234615865843651857942052864
- a[l]"(p[l] - 1) mod p[l];
- 1
- p[2] := nextprime(10~20 + randO);
- p2 := 100000000427419669091
- a[2] : = rand(); # Maple ha3 a 12-digit random number generator:
- a2 := 321110693270
- a[2] mod p[2];
- 321110693270
- a[2]-(p[2] - 1);

Error, integer too large in context

Fermat's discovery of his little theorem was a direct outcome of his investigations concerning Euclid's theorem on perfect numbers. More specifically it originated from his investigations into the question of the primality or otherwise of$(2^n - 1)$.

On occasion we say things to our students like: I'm not sure how such- and-such first happened, was discovered, but I think it happened like this... For example, I find myself telling my students how I think Euclid could have discovered his famous theorem on perfect numbers. Also, many years ago, I used to (wrongly) tell how I thought Fermat had discovered his 'little' theorem... ; I thought he had found it by thinking about the decimal expansions of rational numbers. In Section consider decimal and other expansions, and there you will see how anyone could have formulated Fermat's little theorem had he/she simply asked the right questions having investigated decimal expansions of certain rational numbers.

DECIMAL (AND OTHER) EXPANSIONS OF RATIONAL NUMBERS

Here the simple, and clear point I wish to make isn't just does Fermat's little theorem clarify, or help one to comprehend certain outstanding marvels regarding the decimal expansions of rational numbers, however that those very wonders themselves - with general bases being u»?d (and not simply decimal, for example base 10) - can lead somebody to re-finding of Fermat's little theorem. Specifically, on the off chance that one were working with youthful understudies, at that point, with appropriate direction, they could be directed to guess Fermat's little theorem.

Specifically I refer to the quickly observed fact that the number of digits in the period of the decimal expansion of$\frac{1}{p}$(where p is any prime with$p \neq 2, p \neq 5$) appears to an imestigator to be (and may be proved using Fermat's little theorem to be):

- either (p — 1)
- or a divisor of (p — 1)

<u>Start</u>. Many sensitive young people are fascinated (or, at least, used to be!) with phenomena like:

$\frac{1}{2} = .5$

- $\frac{1}{3} = .33333333$
- ... ad infinitum

$\frac{1}{4} = .25$

- $\frac{1}{5} = .2$
- $\frac{1}{6} = .16666666$
- ... ad infinitum

$\frac{1}{7} = .142857$

- 142857 142857 ... *ad infinitum* [Here, and elsewhere, I make spaces to emphasise the periodic block.]

$\frac{2}{7} = .285714$

285714 285714 ... *ad infinitum and - as almost everyone who has ever investigated such matters (without knowing that it has all already long been discovered) - one quickly finds that*

- the rational number $\frac{m}{n}$(where m and n are positive, m < n) has a *periodic* decimal expansion provided n is not divisible by 2 or 5

$\frac{1}{21} = .47619e\text{-}1$

047619 047619 (I have deliberately made spao?s to emphasise the periodic block) ...

- otherwise $\frac{m}{n}$has an *eventually periodic* decimal expansion

$\frac{1}{22} = .0e\text{-}2$

45 45 45 45 ... (here *n* is divisible by 2)

$\frac{1}{185} = .0e\text{-}2$

054 054 054 ... (here n is divisible by 5)

• Anyone who gets preoccupied with the lengths of these periodic blocks quickly makes an often made (re)discovery: for prime$p$ $(\ p \neq 2,\ p \neq 5)$ the length of the period of the decimal expansion of$\frac{1}{p}$is either (p— 1) or a divisor of (p— 1). A sensitive eye gets quickly drawn towards the 'prime' element in all of this because the examples with long periods - long in relation to the size of the denominator - having encountered examples like:

$\frac{1}{7} = .142857$

142857 142857 ... [period length 6]$\frac{1}{17}$= .5882352941176470©-10 5882352941176 47 ... [period length 16]$\frac{1}{19}$= .5263157894736842le-1 0 526315789473684 21 ... [period length 18] and the other primes p. up to 100. for which$\frac{1}{p}$has period length (p— 1) are 23. 29, 47, 59. 61 and 97. Anyone who knows sufficient Number Theory will know that they are primes p for which ord$_p$(10) = p — 1; in other words they are primes for which 10 is a primitive root [See, too. Section on open problems]. As soon as the eye has got drawn in to$\frac{1}{p}$ for p = 7, 17. 19, 23. 29, etc, then the eye returns to look at the decimal expansions of the reciprocals of the other primes (not 2 or 5), and notices:

$\frac{1}{3} = .3$

3 3 3 3 3 ... [period length 1]$\frac{1}{11}$= .9e-l 09 09 09 09 ... [period length 2] $\frac{1}{13}$= ,76923e-l 076923 076923... [period length 6]= .32258064516129^1 0 32258064516129 ... [period length 15] $\frac{1}{31}$

Maple has a command for computing those periodic decimals expansions, and it'8 called 'pdexpand'. To access it one needs to load Maple's Number Theory package:

- with(numtheory);

Warning, new definition for M

Warning, new definition for order

- *order(10, 7);*
- pdexpand(l/31);

PDEXPAND(1, 0, []. [0. 3, 2. 2. 5, 8. 0. 6, 4, 5. 1, 6, 1, 2, 9])

This is not a Maple tutorial, but anyone who wishes may consult what Maple has to say about "pdexpand" by executing the following line (first remove the and then execute):

- # ?pdexpand
- pdexpand(135/14);

PDEXPAND(1, 9. [6]. [4, 2, 8. 5. 7, 1])

means that $\frac{135}{14}$= 9.6 428571 428571 428571 ... ad infinitum. and

- convert(PDEXPAND(-1, 2, [1, 1], [9, 0, 1, 3]), rational);

$\frac{-1059401}{499950}$

means that -2.11 9013 9013 9013 ... =$-\frac{1059401}{499950}$.

- pdexpand(1/7); PDEXPAND(1, 0, [], (1, 4, 2, 8. 5, 7])
- pdexpand(l/21); PDEXPAND(1, 0, [], [0. 4, 7, 6. 1, 9])
- pdexpand(l/22); PDEXPAND(1, 0. [0], [4. 5])
- pdexpand(1/185); PDEXPAND(1. 0. |0]. [0. 5, 4])

In passing I cannot resist asking if from: $\frac{1}{11}$= .9e-l 0909 09 ... (A) my reader can determine the decimal expansion of $\frac{1}{11^2}$? In other words, what do you get if you square both sides of (A)?

- pdexpand(l/ll); PDEXPAND(1, 0. 0, [0, 9])
- pdexpand(l/ll^2);

PDEXPAND(1, 0. ||, [0, 0. 8. 2, 6. 4. 4, 6. 2. 8, 0, 9. 9, 1, 7. 3, 5, 5. 3, 7, 1. 9|) And $\frac{1}{11^3}$?

- pdexpand(l/ll^3);

```
PDEXPAND(1, 0, [], [0, 0, 0, 7, 5, 1, 3, 1, 4, 8, 0, 0, 9, 0, 1, 5, 7, 7, 7, 6, 1, 0, 8, 1, 8, 9, 3,
3, 1, 3, 2, 9, 8, 2, 7, 1, 9, 7, 5, 9, 5, 7, 9, 2, 6, 3, 7, 1, 1, 4, 9, 5, 1, 1, 6, 4, 5, 3, 7, 9,
4, 1, 3, 9, 7, 4, 4, 5, 5, 2, 9, 6, 7, 6, 9, 3, 4, 6, 3, 5, 6, 1, 2, 3, 2, 1, 5, 6, 2, 7, 3, 4, 7,
8, 5, 8, 7, 5, 2, 8, 1, 7, 4, 3, 0, 5, 0, 3, 3, 8, 0, 9, 1, 6, 6, 0, 4, 0, 5, 7, 0, 9, 9, 9, 2, 4,
8, 6, 8, 5, 1, 9, 9, 0, 9, 8, 4, 2, 2, 2, 3, 8, 9, 1, 8, 1, 0, 6, 6, 8, 6, 7, 0, 1, 7, 2, 8, 0, 2,
4, 0, 4, 2, 0, 7, 3, 6, 2, 8, 8, 5, 0, 4, 8, 8, 3, 5, 4, 6, 2, 0, 5, 8, 6, 0, 2, 5, 5, 4, 4, 7, 0,
3, 2, 3, 0, 6, 5, 3, 6, 4, 3, 8, 7, 6, 7, 8, 4, 3, 7, 2, 6, 5, 2, 1, 4, 1, 2, 4, 7, 1, 8, 2, 5, 6,
9, 4, 9, 6, 6, 1, 9, 0, 8, 3, 3, 9, 5, 9, 4, 2, 9])
```

A suggestion for playing. Much fun may be had by investigating (and explaining what's going on with) decimal expansions of $\frac{1}{101}, \frac{1}{101^2}, \frac{1}{101^3}, \cdots$; $\frac{1}{1001}, \frac{1}{1001^2}, \frac{1}{1001^3}$,... ; etc. A knowledgeable practitioner should be able to quess, and prove results.

A word of warning. One must be careful about saving ones before executing some commands!!

Returning to above. And now to observe the obvious connection to Fermat's little theorem. All, I believe, becomes clear from almost one reflection; simply consider the decimal expansion of, say, $\frac{1}{7}$:

$\frac{1}{7} = .142857$

142857 142857 ... *cut infinitum*

How does one prove that the non-terminating decimal on the right hand side is equal to the (rational) number $\frac{1}{7}$?Of course one needs to have studied infinite series to giw a precis? meaning to such an object...

It's very simple, and straightforward, providing one *knows* that:

$$\sum_{n-1}^{\infty} r^n = \frac{r}{1-r}$$

for $-1 < r < 1$

and thus:

$$.111\ldots\ ad\ infinitum = \sum_{n-1}^{\infty} \left(\frac{1}{10}\right)^n = \frac{1}{10\left(1-\frac{1}{10}\right)} = \frac{1}{10-1} = \frac{1}{9}$$

$$.010101\ldots\ ad\ infinitum = \sum_{n-1}^{\infty} \left(\frac{1}{10^2}\right)^n = \frac{1}{10^2\left(1-\frac{1}{10^2}\right)} = \frac{1}{10^2-1} = \frac{1}{99}$$

$$.001001001\ldots\ ad\ infinitum = \sum_{n-1}^{\infty} \left(\frac{1}{10^3}\right)^n = \frac{1}{10^3\left(1-\frac{1}{10^3}\right)} = \frac{1}{10^3-1} = \frac{1}{999}$$

etc

Two points, now, are simply these:

- Fermat's little theorem (with p = 7, a = 10) forcesto have the decimal (10) expansion that it has. $\frac{1}{7}$
- The decimal expansion of $\frac{1}{7}$, being what it is, forces Fermat's little theorem to hold for p = 7, a = 10.

Why? It's simple;

1. By Fermat's little theorem, with p = 7 and a = 10, we have 10^6 = 1 (mod 7), and thus 7 divides (10^6 — 1). Performing the division by 7 we find that 10^6 - 1 = 7*142857, and so it follows that:

$\frac{1}{7} = \frac{142857}{10^6-1}$

= .142857 142857 142857 ... *cut infinitum*

2. If one has determined that the decimal expansion of i *is* given by:

$\frac{1}{7} = .142857$

142857 142857 ... *ad infinitum*

then one has $\frac{1}{7} = \frac{142857}{10^6-1}$, namely 10^6 - 1 =7*142857. Thus 7 divides (

10^6 - 1), and so it *follows* that 10^6 = 1 (mod 7).

I hardly need write any more on this?

QUADRATIC AND OTHER CONGRUENCES MERSENNE AND FERMAT NUMBERS

Here I begin with a famous empirical discovery of Fermat's:

every odd prime divisor of (x^2 + 1) leaves remainder 1 on division by 4

In the following, this is what I am doing: I first form a random x2 + 1, factor it, and then verify that every odd prime divisor leaves remainder 1 on division by 4. Bear in mind that

- if x is odd then one of the primes dividing x^2 + 1 will be 2 itself (and it is trivial that 22 will not be a factor), otherwise all the other prime factors will be odd (and, in extremis, there might only be one: 3^2 + 1 = 2*5)

- if x is even then all primes dividing x^2 + 1 will be odd (and, in extremis, there might only be one: 2^2 + 1 = 5)

```
> x := rand();

x := 343633073697

> n := x^2 + 1;

n := 118083689338447833247810

> m := ifactor(n);

m := (2) (5) (542340005228713697) (21773)

> L := [op(m)];

L := [ (2), (5), (542340005228713697), (21773)]

> r := nops(L); # how many prime factors there are

r := 4

•         for k to r do

•         p[k] := op(L[k])

•         od;
```

p_4 := 2

p_2 := 5

p_3 := 542340005228713697

p_4 := 21773

```
•         for k to r do

•         p[k] mod 4

•         od;

2

1

1

1
```

All these odd primes (which will change every time the two commands are re-executed) are congruent to 1 mod 4. Euler gave a proof based on Fermat's little theorem.

An extension of that result is that *every* odd prime divisor of (x^4 + 1) leaves remainder 1 on division by 4

Here, numerical experimentation like the above (using rand()) would be problematic, since Maple - almost certainly - would have difficulty in performing the resulting factorisations (and, in fact, it is precisely the difficulty of factoring that is the basis of RSA public-key cryptography).

Instead, I choose more modestly sized n's to factor:

```
•         x := randO mod 1234321; # to reduce the
          3ize of 'x':

x := 57094

•         n := x^4 + 1;

n := 10625806006435226897

•         m := ifactor(n);

m := (17) (718040S874809) (87049)

•         L := [op(m>];

L := | (17). (71804(8874809), (87049)]

•         r := nops(L); # hou many prime factors
there are

r := 3

•         for k to r do

•         p[k] := op(L[k])

•         od;
```

p_1 := 17

p_2 := 718040S874809

p_3 := 87049

```
•         for k to r do

•         p[k] mod 8 # note the change to mod 8

•         od;

1
```

1

1

That result - re (x^4 + 1) - may be proved in the same way as the (x^2 + 1) result. In general one has:

every odd prime divisor of $(x^{(2^m)} + 1)$ leaves remainder 1 on division by $2^{(m+1)}$

This result enables trial factoring of Fermat numbers to be eased, and there is another simple extension of it that saves a further 50%...

Yet another application of Fermat's little theorem is to the trial factoring of Mersenne numbers ($M_p = 2^P$ — 1, with p prime): Theorem. Every prime divisor q of M_p satisfies q = 1 (mod p).

It is pleasing that that Theorem can be proved by using Fermat's little theorem, when it was precisely the very discovery of that theorem which led Fermat to discover his little theorem in the first instance.

Comment. A great deal more about Mersenne numbers (including the Lucas- Lehmer test) is available in my 1995 Maple public lecture "The recently discovered record largest known prime," and a great deal more more about Fermat numbers (including the Pepin test) is available in my 1999 Maple public lec- ture"The history of Fermat numbers from August 1641,* both at my web site.

PRIMALITY TESTING

Here I only remark that the modern study of primality testing really begins with the trail blaising work of Lucas, via Fermat's little theorem, and I urge any serious reader to rush to their bookdealer and obtain a copy of the wonderful book by Hugh C. Williams.

I have briefly hinted at the sort of use that can be made of Fermat's little theorem to establish that a number is composite, but a great deal more is involved in using it as a starting point in proving that a number is prime.

I refer the interested reader to my web site, where I have many Maple worksheets - in the 2nd and 3rd year, and Public and Other Lectures sections of my site's Maple section - devoted to primality testing.

RSA PUBLIC-KEY CRYPTOGRAPHY

Frequently it is (correctly) stated that a fundamental element in the renowned RSA cryptographic method is the use of the Fermat-Euler theorem: let n (1 < n) be a natural number, and a be any integer with god(a, n) = 1, then $a^{\phi(n)} = 1$(mod n), where $\phi(n)$ is the Euler p/ii-function (the number of integers between 1 and n that are relatively prime to n). In fact it is only a very special case of this theorem that is needed for the RSA application, namely the case where n = pq, where p and q are distinct primes (in practical applications p and q are both large, and with some added refinements for security purposes). A fairly detailed exposition of the RSA method may be read in my Maple public lecture - Bill Clinton, Bertie Ahem, and digital signatures - in the Maple Public and Other Lectures section of my web site.

The two prime version of Fermat's little theorem is simply this: let

- *p* and *q* be *distinct* primes (in *cryptographic applications* they will be large, but not just *merely* large (as is sometimes incorrectly stated); to see *why,* refer to Section)

- a be any integer with $a \neq 0$(mod p) and $a \neq 0$(mod q)

then

$a^{((p-1)(q-1))} = 1$

$(\mathrm{mod}\ pq)$

One may easily give a proof of the two prime version which is independent of the normal proof of the full Fermat-Euler result.

Proofs of some important, consequences of Format's 'little' theorem.

Euler's (Ivory's?) proof of Format's little theorem : This proof relies on the simple, but powerful observation that for prime p. and integer $a \neq 0$(mod p), one has

$a\ .\ 1,\ a\ .\ 2,\ a\ .\ 3$

$, \ldots\ a\ .\ (p-2),\ a\ .\ (p-1) = 1,\ 2,\ 3,\ \ldots\ ,\ p-2,\ p-1$(mod p) in some order

A small prime numerical demonstration:

► restart;

► p := 23;

p := 23

► a := 12;

a := 12

► seq(a*k mod p, k=l..p-l);

12. 1, 13. 2, 14. 3. 15. 4. 16. 5. 17, 6. 18, 7. 19, 8. 20, 9. 21, 10. 22, 11

► sort([seq(a*k mod p, k=l..p-l)]);

[1. 2. 3, 4, 5. 6, 7, 9, 10. 11, 12. 13, 14, 15. 16, 17. 18. 19, 20. 21, 22]

Then $a^{(p-1)}(p-1)! = (p-1)!$(mod p), from which it follows that $a^{(p-1)} = 1$

(mod p).

Euler's proof concerning (x^2 + 1) : Suppose $x^2 + 1 = 0$(mod p) for some prime p with p = 3 (mod 4). Then from $x^2 = -1$*(mod* p) *one has* $(x^2)^{(\frac{p-1}{2})} = (-1)^{(\frac{p-1}{2})}$*(mod* p), *giving*

$$x^{(p-1)} = 1$$

$$(\mathrm{mod}\ p) \ldots \ (i)$$

But clearly $x \neq 0$ (mod p), and so by Fermat's little theorem

$$x^{(p-1)} = -1$$

$$(mod\ p) \ldots \ (ii)$$

and (i) and (ii) are incompatible for *odd p,* since they imply 2 = 0 (mod *p).*

An easy proof of a 2-prime version of Fermat's little theorem : If one is in a hurry then this proof allows one to sidestep having to establish all the side work necessary to a proof of the full Euler-Fermat theorem; one merely has to make two applications of the standard Fermat little theorem. We have:

$$a^{(p-1)} = 1$$

$$(\mathrm{mod}\ p)$$

and thus

$$(a^{(p-1)})^{(q-1)} = 1^{(q-1)}$$

$$(\mathrm{mod}\ p)$$

giving

$$a^{((p-1)(q-1))} = 1$$

$$(\mathrm{mod}\ p)$$

Similarly

$$a^{((p-1)(q-1))} = 1$$

$$(\mathrm{mod}\ q)$$

and thus

$$a^{((p-1)(q-1))} = 1$$

$$(\mathrm{mod}\ pq)$$

since gcd(p. *q)* = 1. [End of proof.)

As one quickly learns in RSA public-key cryptography, the 2-prime version of Fermat's 'little' theorem plays a central role.

A GENERALIZATION OF FERMAT'S LITTLE THEOREM

In this lecture, we cover Fermat Little Theorem, Euler's generalization of this theorem, and end with Wilson's theorem. Fermat's Little Theorem, and Euler's theorem are two of the most important theorems of modern number theory. Since it is so fundamental, we take the time to give two proofs of Fermat's theorem: (i) the induction based proof, and (ii) the permutation based proof. The second of these generalizes to give a proof of Euler's theorem. There is a third proof using group theory, but we focus on the two more elementary proofs.

One form of Fermat's Little Theorem states that if p is a prime and if a is an integer then

$$p \mid a^p - a.$$

For example divides 2^3 — 2 = 6 and 3^3 — 3 = 24 and 4^3 — 4 = 60 and 5^3 — 5 = 120. Similarly, 5 divides 2^5 — 2 = 30 and 3^5 — 3 = 240 et cetera.

Obviously a^p — a factors as *a(*$a^{p\text{-}1}$ — 1). So if p \ *a* then we have

$$p \mid a^{p-1} - 1.$$

This gives another common form of Fermat's Little Theorem. For example, divides 5^2 — 1 = 24 and 4^2 — 1 = 15 and 2^2 — 1 = 3. Also, 5 divides 2^4 — 1 = 15 and 3^4 — 1 = 80 and 4^4 — 1 = 255, and 7 divides 2^6 — 1 = 63 et cetera.

After Gauss introduced congruences, the theorem was typically written

$$a^p \equiv a \mod p$$

or, equivalently,

$$a \not\equiv 0 \mod p \implies a^{p-1} \equiv 1 \mod p.$$

Euler phi-function-

In this section Definition, the Euler phi-function is defined as follows.

Definition (Stinson) Suppose $a \geq 1$ and $m \geq 2$ are integers. If gcd(a,m) = 1 then we say that a and m are relatively prime. The number of integers in $\mathbb{Z}_m$ that are relatively prime to m is denoted by $\phi(m)$. We set $\phi(1) \quad 1.$ The function

$$m \mapsto \phi(m), \ m \geq 1$$

is called the Euler phi-function, or Euler totient function. Clearly, for m prime, we have $\phi(m) - m - 1.$ Further, we state the following fact without proof, and leave the proof as an easy exercise.

Fact. If m is a prime power, say, m = p^e, where p is prime and p > 1, then

$$\phi(m) - m(1 - \tfrac{1}{p}) - p^e - p^{e-1}.$$

CONCLUSION

In this paper, we have presented an original proof of Fermat's Little Theorem. The significance of this proof lies in the fact that it relies only on mathematical techniques older than either the statement of the theorem by Fermat or the first proof by Euler. While the work detailed previously show how diverse the proofs of Fermat's Little Theorem can be, it is important to note the theorems' practical applications. In his text, An Introduction to Cryptography.

REFERENCES

1. Burton, David M. (2004). Elementary Number Theory, Third Edition. Wm. C. Brown Publishers.

2. Crandall, R., Dilcher, K., Pomerance, C. (1997). A search for Wieferich and Wilson primes. Math. Comp. 66, pp. 433–449. Lerch Quotients and Primes, Fermat Wilson quotients, and the WW Primes 2, 3, 14771 ,13

3. Dickson, L.E. (1919). History of the Theory of Numbers, vol. 1. Carnegie Institution of Washington, Washington, D. C. (1919); reprinted by Dover, Mineola, NY (2005)

4. Dobson, J.B. (2011). On Lerch's formula for the Fermat quotient (2011, preprint); available at http://arxiv.org/abs/1103.3907

5. Gallian, Joseph A. (2000). Contemporary Abstract Algera, Sixith Edition. D. C. Heath and Company.

6. Glaisher, J.W.L. (1900). A congruence theorem relating to Eulerian numbers and other coefficients. Proc. Lond. Math. Soc. 32, pp. 171–198.

7. Grosswald (2004). Emil Topics from the Theory of Numbers, Second Edition. Birkauser Boston.

8. Guy, R.K. (2004). Unsolved Problems in Number Theory, 3rd ed. Springer, New York

9. Hillman, Abraham P. and Gerald L. (2004). Alexanderson Abstract Algebra A First Undergraduate Course, Fifth Edition. International Thomas Publishing.

10. Lerch, M. (1905). Zur Theorie des Fermatschen Quotienten ap−1−1 p = q(a). Math. Ann. 60, pp. 471–490.

11. Mollin, Richard A. (2001). An Introduction to Cryptography. Chapman & Hall/CRC, Boca Raton.

12. Robbins (2006). Neville Beginning Number Theory, Second Edition. Jones and Bartlett Publishers, Inc., Sudbury, MA.

Corresponding Author

Sikander*

Assistant Professor of Mathematics, A.I.J.H.M. College Rohtak, Haryana, India

sikanderbeniwal2212@gmail.com