Early Proofs of Fermat's Little Theorem and Applications

R.P.Sah[#1], U.N.Roy[#2], A.K.Sah[#3], S.K.Sourabh[#4]
[#1]*Dept of Mathematics, R Lal College, Lakhisarai, Munger, Bihar, India*
[#2]*Dept of Mathematics, BRM College, Munger, Bihar, India*
[#3]*Head, Department of Mathematics, Marwari College, Bhagalpur, Bihar, India*
[#4] *UDCA, T.M. Bhagalpur University, Bhagalpur, Bihar, India*

Abstract

In this paper we study some of the early proofs of Fermat's Little Theorem. Many of the original sources to the proofs of these theorems are obscure. The sequence of the proofs appears chronologically, in order to display how the proofs involved throughout the 17th -21th centuries.

Keywords –*Fermat, Little,terminology, emphasize, sketchy.*

I. INTRODUCTION

Fermat's Little Theorem is one of the jewels of Number Theory and to mark the 400th anniversary of Fermat's birth. This little theorem, which was relatively easy to prove, but it has a vast range of mathematical consequences and one major practical application.Bernhard Frenicle de Bessy dated October 18, 1640; Pierre de Fermat first revealed his result. He did not, however, provide a proof, stating to Frenicle. The first proof of Fermat's Little Theorem was given nearly 100 years later by Euler. Burton also tells us that Leibnitz did not receive this recognition, 'for he left an identical argument in an unpublished manuscript sometime before 1683."

From Beginning Number Theory by Neville Robbins [13, p.102], it is a proof found in many number theory textbooks, and we see later that it is essentially equivalent to Euler's first two proofs.In Dickson's History of the Theory of Numbers [7, Chapter 3], the original works to prove Fermat's Little Theorem are given. Among these proofs, worked by Leibniz, Euler, Lambert, Ivory, and Thue.

Enter Leibniz in 1894 attention was called to a collection of unpublished manuscripts located in the Hanover Library attributed to Gottfried Wilhelm von Leibniz (1646-1716), most famous as one of the creators of calculus as well as for his philosophical theory of monads. We usually do not think of Leibniz as a Pioneer of number theory. However, among his works found in the Hanover Library are results believed to have been attained prior to 1683 which include proofs of Both Fermat's Little Theorem and Wilson's Theorem. Euler's first published proof of Fermat's little theorem before 60 years.

A. *The use of 'little' in the theorem*

When theorem is start, to be called Fermat's little theorem. The question is arise, who first use the word 'Little' in the Fermat's little theorem. Actually not everyone calls it so. In Vol 1 [1919] of Dickson's monumental three volume [History of Mathematics] Theory of Numbers, there is an entire chapter devoted to 'Fermat's and Wilson's Theorems. Hardy and Wright, Davenport, Nagell, simply use 'Fermat's Theorem'. And Sierpinski calls it 'Simple theorem of Fermat' in 1964, a selection of problems in the theory of numbers.

Of course everyone knows that Wilson's theorem is only one such theorem but 'Fermat's theorem. There are several claimants to find the beautiful result –to name but one- that every prime p, with p = 1 (mod 4), is represent table by $\mathrm{p} = \mathrm{a}^2 + \mathrm{b}^2$ for some integers a andb, could well claim to be Fermat's theorem.

B. *Fermat's 'little' Theorem with Examples*

If p be a prime and a be any integer then the number $\mathrm{a}^{\mathrm{p}} - \mathrm{a}$ is an integer multiple of p. It is expressed in modular arithmetic as

$$\mathrm{a}^{\mathrm{p}} \equiv \mathrm{a}(\mathrm{mod}\ \mathrm{p})$$

For example: If a= 2, p = 7, 2^7 = 128 and 128 – 2 = 7× 18 is an integer multiple of 7.

In non-congruence language: Let p be any prime, and a be any integer not divisible by p, then $\mathrm{a}^{(\mathrm{p}-1)}$ leaves remainder 1 on division by p. Symbolically,

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

Illustration: Let p =7 and a=2, then $a^{(p-1)} = 2^6 = 64 = 7 \times 9 + 1$.

1) ***Theorem***:Let k be the order of a in the group $\mathrm{Z}_\mathrm{p}^\mathrm{x}$ Then by Lagrange, k divides the order of the group (p – 1) .

So, $p - 1 = km$, for some m.

A more general result is $X^{\alpha(N)} \equiv 1$(mod N), for X and N coprime, where α(N)Euler's function is, the number of integers strictly smaller than N coprime to N. Elegant group-theoretic proof too.

$$a^{p-1} \equiv a^{km} \equiv \left(a^{k}\right)^{m} \equiv 1^{m} \equiv 1 \text{ (mod p)}$$

The following proof is given Beginning Number Theory by Neville Robbins [13, p.102]. It is a proof found in many number theory textbooks, and we see later that it is essentially equivalent to Euler's first two proofs.

Proof: Let $S = \{a|a^p \equiv a\ (mod\ \text{p})\}$ for p prime and a ∈ N. Then 0∈ S because $0^p = 0$ for all p. So $0^p \equiv 0$ (mod p).

Now assume $k \in S$ and $k^p \equiv k$ $(modp)$.

Then we want to show that for $k + 1 \in S$,

$$(k+1)^p \equiv (k+1)(modp).$$

By Binomial Theorem,$(k+1)^p = (k)^p + 1^p + \sum_{j=1}^{p-1} \binom{p}{j} (k)^{p-j}$

$\equiv (k+1)\ (mod\ \text{p})$

If gcd $(a,p) = 1$, then by cancellation $a^p \equiv a\ (mod\ p)$, implies $a^{p-1} \equiv 1\ (mod\ p)$.

If a is negative, then $a \equiv r\ (mod\ p)$ for some r, where $0 \le r \le p - 1$.

Thus $a^p \equiv r^p \equiv r \equiv a\ (mod\ p)$.

2) ***Theorem:***Let p be a prime and let $x = a_1 + a_2 + \cdots + a_m$.and a number$x^p - \sum_{i-1}^{m} a_i{}^p$, show that $p|\ (x^p - \sum_{i}^{m}{}_{1}\, a_i{}^p)$.

Proof:We know by the Multinomial Theorem,

$$x^p = (a_1 + a_2 + \cdots + a_m)^p = \sum_{k_1+\cdots+k_m=p} \binom{p}{k_1, k_2, \ldots, k_m} a_1{}^{k_1}.a_2{}^{k_2} \ldots a_m{}^{k_m}.$$

where$\binom{p}{k_1,k_2,\ldots,k_m} = \frac{p!}{k_1!\ldots k_m!}$, when $k_i \neq p$ for any i, then $k_i < p$ for all i. Then there is no factor of p in the denominator of any coefficient, but there is a factor of p in the numerator. Thus for $k_i \neq p$ for all i, $\frac{p!}{k_1!\ldots k_m!} \equiv 0\ (mod\ p)$.Thus

$$x^p - \sum_{i=1}^{m} a_i{}^p \equiv (a_1{}^p + a_2{}^p \ldots + a_m{}^p) - (a_1{}^p + a_2{}^p \ldots + a_m{}^p)$$

$$\equiv 0 (mod\ p)$$

Thus

$$p|x^p - \sum_{i=1}^{m} a_i{}^p$$

Taking, $a_1 = a_2 = \cdots = a_m = 1$. Then since $x = a_1 + a_2 + \cdots + a_m$, it follows that $p|(x^p - x)$, for any integer x (depending on the value of m). Thus $x^p - x \equiv 0\ (mod\ p)$,

So$x^p \equiv x\ (mod\ p)$. If gcd (x,p)= 1, then by cancellation

$$x^{p-1} \equiv 1\ (mod\ p).$$

C. Euler's Proof with help of Fermat's Little theorem

Fermat's little theorem is an important property of integers to a prime modulus.

For prime p an any a∈ Z such that

$$a \not\equiv 0(\ mod\ p),\quad a^{p-1} \equiv 1(\ mod\ p).$$

If we want to extend Fermat's little theorem to a composite modulus, a false generalization would be: if $a \not\equiv 0$ (mod m) then $a^{m-1} \equiv 1\ (mod\ m)$. For a counter example, take m = 15 and a=2:

$2^{14} \equiv 4 \not\equiv 1$(mod 15).

A correct extension of Fermat's little theorem to non-prime module requires a new way of thinking about the hypothesis in Fermat's little theorem. For prime p,$a \not\equiv 0$ (mod p), $gcd(a, p) = 1$.

But these two conditions are not equivalent when p is replaced with a composite number. It is the relative primarily point of view on the right that lets Fermat's little theorem be extended to a general modulus, as Euler discovered.

1) ***Theorem:***For $m \geq 2$ in $Z^+$and any a∈Zsuch that $(a ,m) = 1$,

$$a^{\varphi(m)} \equiv 1 \text{ (mod } m)$$

Where $\varphi(m)$ is the number of invertible integers modulo m.

When $m = p$ is prime, all non-zero integers modulo p are invertible, So $\varphi(p) = p - 1$ and Euler's theorem becomes Fermat's little theorem.

Now we compute $\varphi(m)$. Consider $m = 12$. To count the number of invertible integers modulo 12, write down a set of representatives for integers modulo 12, such as

$$1,2,3,4,5,6,7,8,9,10,11,12.$$

The numbers here which are invertible modulo 12 are 1,5,7,11,

So $\varphi(12) = 4$.

From Euler's theorem for $m = 12$ says $a^4 \equiv 1$ $(mod\ 12)$ when $(a, 12) = 1$.

Being invertible modulo m is the same as being relatively prime to m, i.e. we can solve $ax \equiv 1$ (mod m) for x, exactly when $(a, m) = 1$, so we can describe $\varphi(m)$ concretely as follows: $\varphi(m) = \{ a{:}1 \leq a \leq m,(a,m) = 1 \}$.

Here is a small table of values derived from this formula.

m	2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
φ(m)	1 2 2 4 2 6 4 6 4 10 4 12 6 8 8 16

where φ(m) is even for $m > 2$.

We can explain this by observing that when a mod m is invertible, so is $(-a)$ mod m. Therefore, using the standard representatives modulo m, invertible numbers modulo m come in pairs as $\{a, m - a\}$.

Suppose $a = m - a$, then $a = m/2$, so m is even.

But $(m/2, m) = m/2$, and this is bigger than 1 when $m > 2$, so $m/2$ is not invertible modulo m. Thus, when $m > 2$, the invertible numbers modulo m fall into pairs, and that shows $\varphi(m)$ is even.

2) ***Theorem***:If a prime$p$ and $a \not\equiv 0$ *mod p*. To show $a^{p-1} \equiv 1$ *mod p*, consider non-zero integers modulo p in the standard range:

$$S = \{1,2,3,\ldots,p-1\}$$

We will compare S with the set obtained by multiplying the elements of S by a:

$$a^S = \{ a^1, a^2, a^{\cdot 3}, \ldots, a^{(p-1)} \}.$$

The elements of S represent the nonzero numbers modulo p. The key point is that the elements of a^Salso represent the nonzero numbers modulo p. For any $b \not\equiv 0$ mod p, we can solve the equation $ax \equiv b$ mod p since a mod p is inventible and a solution x is nonzero modulo p too (since b mod p is nonzero). Choosing z to lie between 1 and p-*1*,$ax \in a^S$, so b mod p is represented by an element of a^S. There are$p$ *-1* elements in a^S, so a^S is a set of representatives for the nonzero numbers modulo p.

Since S and a^S, when reduced modulo p, becomes the same thing, the product of the numbers in each set must be the same modulo p:

$1.2.3\ldots\ldots(p - 1) \equiv a(a.2)(a.3)\ldots(a(p - 1))$ *mod p.*

Pulling the $(p - 1)$ copies of a to the front of the product on the right, we get

$$1.2.3 \ldots\ldots (p - 1) \equiv a^{p-1}(1.2.3 \ldots\ldots (p-1) mod\ p$$

Now we cancel each of $1,2,3,\ldots p - 1$ on both sides (since they are all invertible modulo p) and we are left with$1 \equiv a^{p-1}$ *(mod p).*

3) ***Theorem:***Replace the condition "non-zero modulo p" with "relatively prime to m." For positive integer m and a that $(a,m) = 1$.

We consider the units modulo m in the standard range:

$$\mathrm{S} = \{\mathrm{u}_1.\mathrm{u}_2.\mathrm{u}_3 \ldots\ldots \mathrm{u}_{\varphi(\mathrm{m})}\}.$$

Where $1 \leq u_i \leq m-1, (u_i, m) = 1$, and the u_j's are distinct. (If $m=p$ is prime we can use $\mathrm{u}_i = i$ for all i, but in general there isn't a simple formula for the ith unit modulo m.) We will compare S with the set obtained by multiplying the elements of S by a:

$$aS = \{au_1.au_2.au_3 \ldots\ldots au_{\varphi(\mathrm{m})}\}.$$

Since $(a,m)=1a$ mod m is a unit and therefore a S consists of units modulo m. We will show that a^S represents all the units modulo m. Given any unit b mod m, the congruence $ax \equiv b(\mathrm{mod}m)$ is solvable since a mod m is invertible. The solution x is a unit modulo m and placing x between 1 and $m - 1$ makes ax a member of a^S. Thus b mod m is represented by an element of a^S. Since a^S has size φ(m), it is a set of representatives for the units modulo m.

Since the members of S and a^S agree modulo m, the product of the numbers in each set must be the same modulo m:

$$u_1u_2u_3u_{\varphi(\mathrm{m})} \equiv (au_1)(au_2)(au_3)(au_{\varphi(\mathrm{m})})mod\ m.$$

Pulling the φ(m) copies of a to the product on the right, we get

$$u_1u_2u_3 \ldots . u_{\varphi(\mathrm{m})} \equiv a^{\varphi(\mathrm{m})}u_1u_2u_3 \ldots . u_{\varphi(\mathrm{m})}mod\ m.$$

Now we cancel each U_i on both sides (since they are all invertible modulo m) and we are left with $1 \equiv a^{\varphi(m)}$ mod m.

Passing from Fermat's little theorem to Euler's theorem amounted to replacing non-zero numbers modulo *a* prime *p* with invertible numbers (not the non-zero numbers) for a general modulus *m*. There is a common notation for these numbers in elementary number theory courses.

$$U_m = \{a \; mod \; m : (a, m) = 1\}$$

The notation U_m comes the fact that invertible numbers mod m are called units mod m.

Example: We have $U_5 = \{1, 2, 3, 4\}$ and $U_{18} = \{1, 5, 7, 11, 13, 17\}$.

When *p* is$U_p = \{1, 2, 3, \ldots, p-1\}$.

The functionφ(m) does not vary in a simple manner from one integer to the next. This is typical of functions that arise in number theory which are based on divisibility. The right way to think about φ(m) is by thinking about positive integers not in terms of the usual *m* → *m*+1 paradigm, but in terms of the progression

Primes →prime powers→ general case.

This progression is how the integers are best arranged from the viewpoint of divisibility Primes are the building we can get formulas for φ(*m*)directly from its definition in the first two cases of the above progression:

- φ(*p*)=*p* – 1 since there are *p* – 1 integers from 1 to *p* which are relatively prime to *p*.
- $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ for prime p and *k*≥1 since among the integers from 1 to p^k, those which are not relatively prime to p^k are the multiples of *p: p*, p^2, p^3,…p^k

There are p^{k-1} such numbers, so we subtract this fromp^k to compute

$\varphi(p^k) = p^k - p^{k-1}$.

What about φ(m) when m is composite? We will treat one case here, which is important in elementary cryptography: *m*= *pq* is a product of two different primes. If$1 \le a \le pq$and (*a*, *pq*) =1, then *a* is neither a multiple of *p* nor a multiple of *q*. The multiples of *p* in this range are *p*, 2*p,…,qp* and the multiples of *q* in this range are *q*, 2*q,….pq*. There are *q* numbers in the first case and *p* numbers in the second case. The two lists only overlap at *pq*(indeed, a positive integer divisible by *p* and *q* is divisible by *pq*, so can't be less than *pq*). Therefore, to compute φ(*pq*), we take away from *pq* the number of terms in both lists without double-counting the common term:

$$\varphi(pq) = pq - p - q + 1 = p(q - 1) - 1(q - 1) = (p - 1)(q - 1)$$

This is interesting: φ(*pq*) = φ(*p*)φ(*q*) for different primes *p* and *q*. This formula is false when $p = q$, $\varphi(p^2) = p^2 - p = p(p-1)$ rather than $(p-1)^2$

With these formulas, we can make Euler's theorem more explicit for certain modulo.

Example: When p is prime,

$$(a, p^2) = 1 \Longrightarrow a^{p(p-1)} \equiv 1 \text{ mod } p^2$$

Example*:* When *p* and *q* are different primes,

$$(a, pq) = 1 \Longrightarrow a^{p(p-1)(q-1)} \equiv 1 \text{ mod } pq$$

Example will be crucial for the RSA cryptosystem.

4) ***Theorem:***Any reduced form fraction *a/b* with (10, *b*) = 1 can be written as a fraction with denominator 10^d- 1for some≥ 1. Moreover, the period length of the decimal expansion for *a/b* is the smallest $d \ge 1$ such that $10^d \equiv 1$(mod *b*). In particular, $d \le \varphi(b)$ and the period length is independent of the numerator *a*.

Proof: Let the fraction be *a/b*, where (10, *b*) = 1. By Euler's theorem, $10^{\varphi(b)} \equiv 1$ (mod *b*).

That means $10^{\varphi(b)}$–1 is a multiple of *b*, so we can rewrite *a/b* asa fraction with denominator $10^{\varphi(b)}$ – 1.

Let $d \ge 1$ be minimal such that $10^d \equiv 1$(mod *b*), so $d \le \varphi(b)$. Write 10^d-1 = *bn*, so

$$\frac{a}{b} = \frac{an}{bn} = \frac{an}{10^d - 1}.$$

Since *a/b* <1, *an* <*bn* = 10^d- *1*. Therefore the base 10 expansion of an requires no more than *d* digits, so we can write *a.n* = $c_2 10^{d-1} + c_2 10^{d-2} + \ldots \ldots + c_d$ for some digits $c_{i.}$ (Some of the top c_i's may be 0 if an is substantially less than 10^d- 1.)

Our earlier calculations showed that for any decimal digits$c_1, \ldots, c_d$,

$$.\overline{c_1 c_2 \ldots c_d} = \frac{c_1 10^{d-1} | c_2 10^{d-2} | \ldots . | c_d}{10^d - 1}$$

So,*a/b* = $(c_1 10^{d-1} + \cdots + c_d)/(10^d - 1)$has a periodic decimal expansion of length *d*.

Example: A numerical computation suggests the decimal expansions of 1/7,2/7,3/7,4/7,5/7 and 6/7 all have period length 6 and the decimal expansions of 1/303 and 28/303 both have period length 4. To prove this, check the least d such that $10^d \equiv 1$ mod 7 is 6 and the least *d* such that $10^d \equiv 1$ mod 303 is 4.

By seeing explicitly$10^6 \equiv 1$ is a multiple of 7 and $10^4 \equiv 1$ is a multiple of 303, we take even figure then the decimal expansions of these fractions are since$10^6 \equiv 1 = 7.142857,$

$$\frac{3}{7} = \frac{3.142857}{10^6 - 1} = \frac{428571}{10^6 - 1} = 428571428571 \ldots$$

Since $10^4 - 1 = 303.33,$

$$\frac{28}{303} = \frac{28.33}{10^4 - 1} = \frac{924}{9999} = .092409240924 \ldots$$

The whole theory of periodic decimal is explained by Euler's theorem and results related to it. So this is a concrete elementary application of number theory to explain a persistent mystery from mathematics familiar to all students.

The requirement if theorem that a/b lie between 0 and 1 is a red herring. This is best explained by an example. Consider 1543/303. To find its decimal expansion, we first extract the integer part. Since 1543 = 303 – 5 + 28, 1543/303 = 5 + 28/303. So the decimal part of 1543 / 303 is the same as that of 28 / 303, which lies between 0 and 1. Now we can apply Theorem.

Since 28/303 = .092409240924…,
1543/303=5.092409240924…..

In general, check that for any reduced form fraction *a/b*> 1, subtracting its integer part leaves a fraction between 0 and 1 which still has b as its reduced form denominator, so the period of the decimal expansion of *a/b* is still completely determined by *b*.

There are further interesting questions worth asking about decimal expansions:

- Which numbers have finite decimal expansions (such as 5/16=.3125).
- Which numbers have periodic decimal expansions with an initial non repeating block (such as 7/15=.466666…).
- If we compare all the reduced proper fractions with the same denominator *b*, they may all have the same expansion as 1/*b* except for a shift, e.g.

$$1/7 = .\overline{142857},$$
$$2/7 = .\overline{285714},$$
$$3/7 = .\overline{428571},$$
$$4/7 = .\overline{571428},$$
$$5/7 = .\overline{714285},$$
$$6/7 = .\overline{857142},$$

We can explain when all the reduced fractions with denominator *b* have this feature.For some denominators, more than one digit sequence occurs.

e.g., there are two possibilities when the denominator is 13:

$$\frac{1}{13} = .\overline{076923},$$
$$2/13 = .\overline{153846},$$
$$3/13 = .\overline{230769},$$
$$4/13 = .\overline{307692},$$
$$5/13 = .\overline{384615},$$
$$6/13 = .\overline{461538},$$
$$7/13 = .\overline{538461},$$
$$8/13 = .\overline{615384},$$
$$9/13 = .\overline{692307},$$
$$10/13 = .\overline{769230},$$
$$11/13 = .\overline{846153},$$
$$12/13 = .\overline{923076},$$

Every decimal expansion here is a shift of the expansion for 1/13 or 2/13. If we collect numerators of fractions above whose decimal expansions have the same digit sequence, the 12 numerators fall into two sets of size 6: {1,3,4,9,10,12} and {2,5,6,7,8,11}.

II. CONCLUSION

In this paper we have discussed some of the early proofs of Fermat's Little Theorem. We have also demonstrated the Fermat's Little Theorem through examples.

REFERENCES

[1] Hardy, G. H. and Wright, E. M. An Introduction to the Theory of Numbers, 5th ed. Oxford, England: Clarendon Press, 1979.

[2] Nagell, T. "Fermat's Theorem and Its Generalization by Euler." Introduction to Number Theory. New York: Wiley, pp. 71-73, 1951.
[3] Springer Science+BusineHazewinkel, Michiel, ed. (2001) [1994], "Fermat's little theorem", Encyclopedia of MathematicssSéroul, R. "The Theorems of Fermat and Euler." Programming for Mathematicians. Berlin:
[4] Edwards, Harold M., Fermat’s Last Theorem (A Genetic Introduction to Algebraic Number Theory). Springer-Verlag (1977).
[5] Media B.V. / Springer-Verlag, p. 15, 2000.
[6] Dickson, Leonard E. D., History of the Theory of Numbers, Volume 1 (First published in 1919). Chelsea Publishing Company (1971).
[7] Kluwer Academic Publishers, ISBN 978-1-55608-010-4
[8] Albert, A. Adrian (2015) [1938], Modern higher algebra, Cambridge UniversityPress, ISBN 978-1-107-54462-8.
[9] Burton, David M. (2011), The History of Mathematics / An Introduction (7th ed.), McGraw-Hill, ISBN 978-0-07-338315-6