Beyond the Limits of Fermat's and Euler's Theorems

Zuonaki Ongodiebi[1] and Tom Otobong[2] and [3] Udeme O. Ini
[1, 3]Department of Mathematics and Computer Science, Niger Delta University Amassoma, Bayelsa State
[2]Department of Mathematics, Michael Okpara University of Agriculture, Umudike, Abia State

***Abstract*:- We have shown that beyond the limits of Fermat's and Euler's theorems, there is a ray of hope to ascertain the remainder when a number n divides a huge number a . Few illustrative examples are solved and a new relevant proposition is given.**

Key words: Modulo, Congruence, Co-prime, residue.

1. INTRODUCTION

Fermat's and Euler's theorems are useful in finding solutions to linear and nonlinear congruences Eugen (2006) and Joshi (2011). See Adel (2018) and Vishnu (2018) for further details; since they provide easy methods to determine the remainder when a number n divides another number say a if certain conditions or restrictions are met . These restrictions are stated in theorems 3.1 and 3.2. Recently, Brierly et.al (2019) and Saimir (2018) have provided proofs of Fermat's last theorem as well as Fermat's conjecture in the domain of natural numbers. The condition when the given problem do not satisfy the conditions of Fermat's and Euler's theorems have never been reported in literature; thereby, motivating this research. Here, we have provided solutions to problems that do not satisfy the conditions of Fermat's and Euler's theorems.

2. PRELININARIES

For a given integer m in □ ; let $\square(m)$ denotes the set $\{0,1,2,\ldots,m-1\}$. The set $\square(m)$ is also known as the set of all remainders (or residues) modulo m .

2.1 Let m and n be integers, where m is positive. Then by remainder's theorem, we can write

$$n = qm + r \qquad (1)$$

where $0 \le r \le m$ and q is an integer. Equation (1) can be interpreted in the language of congruence which means that n is congruent to r modulo m for some integer q ; denoted by $n \equiv r(\bmod m)$.

Definition 2.1: If m is a positive integer and a, b are in □ , then we say that a is congruence to b modulo m (written as $a \equiv b(\bmod m)$), if $a-b$ is divisible by m .

Definition 2.2: An integer a is said to be co-prime (or relatively prime) to another integer b if the greatest common divisor (g.c.d) of a and b is 1 that is $\gcd(a,b)=1$

For example 8 is co-prime to 35, etc. The integer 1 is co-prime to every integer in □ .

Remark 2.1: If m is a prime number, then every non-zero element of $\square(m)$ is co- prime to m .

Definition 2.3: Let n is a positive integer and $\square(n)$ as defined above. Let $\square^{(x,n)}(n) = \{x : (x,n) = 1, x \in \square(n)\}$. Then the cardinal number of $\square^{(x,n)}(n)$ is denoted by $\phi(n)$. The function ϕ is called Euler's phi function.

For example $\phi(8) = 4,\ \phi(7) = 6,$ etc. In general, for any prime p , $\phi(p) = p-1$

Properties of Congruence

For any integers a and b and a positive integer n, we have the following:

(i) $a \equiv b \bmod n$ **(reflexive)**

(ii) If $a \equiv b \bmod n$, then $b \equiv a \bmod n$ **(symmetric)**

(iii) If $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$ **(transitive)**

(iv) If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $a + c \equiv b + d \bmod n$ also, $ac \equiv bd \bmod n$

3. ILLUSTRATIVE EXAMPLES:

We know that $23 \equiv 2 \bmod 7$. By squaring this, we have

$23^2 \equiv 4 \bmod 7$ and also $23^3 \equiv 8 \bmod 7 \equiv 1 \bmod 7$ by transitive property stated above. With that above process, it becomes easy to find remainders of huge numbers.

Example 1: Find the remainder when 19^{139} is divided by 10.

Solution: Note that $19 \equiv 9 \bmod 10$

$$19^2 \equiv 81 \bmod 10 \equiv 1 \bmod 10$$

now $(19^2)^{69} = 19^{138} \equiv 1 \bmod 10$. Therefore,

$$19^{138} \times 19 \equiv 1 \times 9 \bmod 10$$

that is $19^{139} \equiv 9 \bmod 10$ $\therefore$ the remainder is 9. Pretty simple!

Example 2: Determine the remainder when 22^{738} is divided by 17.

Solution: $22 \equiv 5 \bmod 17$

$$22^2 \equiv 25 \bmod 17 \equiv 8 \bmod 17$$

$$22^3 \equiv 125 \bmod 17 \equiv 6 \bmod 17$$

$$22^4 \equiv 625 \bmod 17 \equiv 13 \bmod 17$$

Proceeding in this form will lead us to frustration, and as a result, we present the following theorem.

Theorem 3. 1 (Fermat's Theorem)

If $a \in Z$ and p is a prime not dividing a, then p divides $a^{p-1} - 1$. That is $a^{p-1} \equiv 1 \bmod p$ for a $\text{not} \equiv 0 \bmod p$.

Applying Fermat's theorem to example 2, we have that $a = 22$ and $p = 17$. Thus

$$a^{p-1} \equiv 1 \bmod 17$$

$$22^{16} \equiv 1 \bmod 17$$

$(22^{16})^{46} = 22^{736} \equiv 1 \bmod 17$ and

$$22^2 \equiv 8 \bmod 17$$

$$\therefore\ 22^{738} \equiv 8 \bmod 17$$

Therefore, the remainder is 8.

Suppose in example 2 above, the modulus was 15; that is $22^{738} \bmod 15$ then Fermat's theorem fails to provide solution since 15 is not a prime number. To handle such problems, consider the following theorem.

Theorem 3.2 (Euler's Theorem)

If a is an integer relatively prime to n, then $a^{\phi(n)} - 1$ is divisible by n. That is

$$a^{\phi(n)} \equiv 1 \bmod n$$

Example 3: Use Euler's theorem to find the remainder when 22^{738} is divided by 15.

Solution: Since the $\gcd(22,15) = 1$, Euler's theorem is applicable. Now $a = 22,\ n = 15$ and $\phi(n) = 8$. It follows that

$$22^8 \equiv 1 \bmod 15$$

$(22^8)^{92} = 22^{736} \equiv 1 \bmod 15$ and

$$22 \equiv 7 \bmod 15$$

$$22^2 \equiv 49 \bmod 15 \equiv 4 \bmod 15$$

$\therefore\ 22^{738} \equiv 4 \bmod 15$ leaving a remainder 4

Example 3: Determine the remainder when 3^{54} is divided by 66. In this example, 66 is not a prime number which implies that Fermat's theorem can not be applied. Also the $\gcd(3,66)=3$ which obviously means 3 and 66 are not relatively prime and as a result, Euler's theorem cannot be applied! What next?

To solve the above problem, let us first consider a simple version of the given problem: Find the remainder when 3^4 is divided by 66 i.e $3^4 \bmod 66$.

Clearly $3^4 = 81 \equiv 15 \bmod 66$; thus the remainder is 15. Alternatively, $a=3$ and $n=66$. By division of $3^4 \bmod 66$ by 3 gives

$$3^3 \bmod 22 \Rightarrow 3^3 = 27 \equiv 5 \bmod 22 \qquad (3.1)$$

Now multiply through the congruence (3.1) by $a=3$;

i.e $3\times 3^3 \equiv 3\times 5 \bmod 3\times 22$ or $3^4 \equiv 15 \bmod 66$ which also results to the same remainder.

With this ray of hope, let us solve example 3.

The given problem is

$3^{54} \bmod 66$. By dividing through by 3, we have

$3^{53} \bmod 22$. At the point, we can now apply Euler's theorem since 3 and 22 are relatively prime. Thus

$$3^{\phi(22)} = 3^{10} \equiv 1 \bmod 22$$

$$3^{50} \equiv 1 \bmod 22$$

$$3^3 \equiv 5 \bmod 22$$

$$3^{53} \equiv 5 \bmod 22$$

$\therefore\ 3^{54} \equiv 15 \bmod 66$. Thus the remainder is 15.

Remarks: It is a mere coincidence that $3^4 \bmod 66$ and $3^{54} \bmod 66$ have the same remainder. The example we considered, observe that $n > a$.

Example 4: Find the remainder when 25^{41} is divided by 15.

Solution: Again, 15 is not a prime number and as such, Fermat's theorem can not be applied. Also, the $\gcd(25,15) > 1$ which violates Euler's theorem.

The given problem is

$25^{41} \bmod 15$

Divide through by 5

$5^{81} \bmod 3$

Now since the $\gcd(3,5)=1$ and also 3 is prime, we can apply either Fermat's or Euler's theorems. By applying Fermat's theorem, we have

$5^{80} \equiv 1 \bmod 3$ and since $5 \equiv 2 \bmod 3$;

we have

$5^{81} \equiv 2 \bmod 3$

at this point, we multiply through by 5

$5^{82} \equiv 10 \bmod 15$ or

$25^{41} \equiv 10 \bmod 15$. Thus the remainder is 10.

Remark: Observe that in this example, $n < a$. Thus we state the following proposition.

Proposition 3.1

Suppose a and n are integers and n in not a prime; and suppose also that $\gcd(a,n) > 1$, then the remainder when a^m is divided by n is given by

$$r = \begin{cases} a\{a^{m-1} \bmod (n/a)\} & \text{if n > a} \\ \gcd(a,n)\{\dfrac{a^m}{\gcd(a,n)} \bmod (\dfrac{n}{\gcd(a,n)})\} & \text{if n < a} \end{cases}$$

4. CONCLUSION

We have shown that the remainder when a number n divides another number say a can be easily determined even if it does not satisfy the criteria for both Fermat's and Euler's theorems. We demonstrate our claim with relevant examples.

5. REFERENCES

[1] Adel, Betina and Emmanuel, Lecouturier, Congruence formulas for Legendre modular polynomials. *Journal of Number Theory*, Vol 188, 2018 71-87

[2] Eugen Vedral, Solutions of Some Classes of Congruences, *The Teaching of Mathematiccs*, Vol. IX, 2006, 41-44.

[3] J. E. Briervely, Takashin, Ito and Hidegoro Nakano, *A simply proof of Fermat's last theorem*. Scholar Journal of Applied Sciences and Research, Vol. 2, 2019; 1- 4

[4] K. Vishinu Namboothin, On the number of solutions of a restricted linear congruence

[5] *Journal of Number Theory*, Vol 188, 2018; 324-334

[6] S. R. Joshi, Nonlinear Congruences in the Theory of Numbers, *Bulletin of the Marathwada Mathematical Society*, Vol. 12, 2011, 24-31.

[7] Saimir, A. Lolja, *The proof of the Fermat's conjecture in the correct domain*. Vol. 35, 2018; 53- 74