International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-10, Issue-2, March 2022
https://doi.org/10.55524/ijircst.2022.10.2.2
Article ID IRP1247, Pages 7-9
www.ijircst.org

Application of Fermat's Little Theorem in Congruence Relation Modulo n

S. P. Behera[1], J. K. Pati[2], S. K. Patra[3], and P. K. Raut[4]

[1]Assistant Professor of Mathematics, C.V.Raman Global University, Bhubaneswar, Odisha, India
[2]Associate Professor of Mathematics, C.V.Raman Global University, Bhubaneswar, Odisha, India
[3]MSc Project Scholar, C.V. Raman Global University, Bhubaneswar, Odisha, India
[4]Research Scholar, C.V. Raman Global University, Bhubaneswar, Odisha, India

Correspondence should be addressed to S.P. Behera; sivaiitkgp12@gmail.com

ABSTRACT- According to Fermat's little theorem, for any p is a prime integer and $gcd(x,p)=1$, then the congruence $x^{p-1}\equiv 1(mod\ n)$is true, if we remove the restriction that $gcd(x,p)=1$, we may declare$x^{p-1}\equiv x(mod\ p)$. For every integer x. Euler extended Fermat's Theorem as follows: if $gcd(x,p)=1$,then,where $x^{\phi(n)}\equiv 1(mod\ n)$.$\phi$ is Euler's phi-function.
Euler's theorem cannot be implemented for any every integers x in the same manners as Fermat's theorem works; that is, the congruence $x^{\phi(n)+1}\equiv x(mod\ n)$ is not always true. In this paper, we discussed the validation of congruence $x^{\phi(n)+1}\equiv x(mod\ n)$.

KEYWORDS- Chinese Remainder theorem, Euler's Function, Fermat's little theorem, Primitive Roots

I. INTRODUCTION

For any p is a prime number the Fermat's little theorem state that, then $\gcd(x,p)=1$ and$x^{p-1}\equiv x(mod\ p)$. We may say$x^{p}\equiv x(mod\ p)$. For any integer x if the constraint$\gcd(x,p)=1$ is lifted. This last congruence will be referred to as a generalization form of Fermat's little theorem.
Euler generalized Fermat's theorem as follows. If $\gcd(x,p)=1$,$x^{\phi(n)}1(mod\ p)$, where ϕ is Euler's phi function[2]. Obviously, like Fermat's theorem, Euler's result cannot be extended to all integers x. In other words, congruence $x^{\phi(n)+1}\equiv x(mod\ n)$ is not always valid. For example, if n = 10, then congruence holds for all values of x, but if n = 12, x = 2, 6, and 10 fail.
In this paper, we explore the following question: for what values of x is the congruence $x^{\phi(n)+1}\equiv x(mod\ n)$valid, given any natural integer n with n>1.When n is a prime number, this congruence is an extension of Fermat's Little Theorem and holds true for all x.
The authors believe that the results would be ideal issues to present in an introductory number theory course because they require just simple methods to show. This paper's terminology may be found in ([1]).

II. THE GENERALIZATION

CASE 1 :(n is prime)

THEOREM- Let P is a prime number, then show that when the congruence $x^{\phi(n)+1}\equiv x(mod\ p)$ is valid, when n is prime.

PROOF
If n is prime then

$$\phi(n)\equiv n-1$$

Euler's generalization form it becomes

$$x^{\phi(n)}\equiv 1(mod\ n)$$

From Fermat's little theorem, we know that

$$x^{n-1}\equiv 1(mod\ p)\quad [When\ n\ is\ a\ prime],[\gcd(x,n=1]$$

Here we have,

$$(x_1+x_2)^n(x)=\left[x_1^n+\binom{n}{1}x_1^{n-1}x_2+\binom{n}{2}x_1^{n-1}x_2^2+\cdots+\binom{n}{n}x_1^{n-n}x_2^n\right](x)$$
$$=[x_1^n+x_2^n\ terms\ divisible\ (by\ n)](x)$$
$$\Rightarrow[(x_1+x_n)^n-(x_1^n+x_2^n)](x)$$
$$=((x)\ terms\ divisible\ by\ n)$$
$$\Rightarrow(x_1+x_n)^n(x)\equiv(x_1^n+x_2^n)(x)(mod\ n)$$
$$\Rightarrow(x_1+x_2+\cdots+x_n)^n(x)$$
$$\equiv(x_1^n+x_2^n+\cdots+x_2^n)(x)(mod\ n)$$

Putting $x_1=x_2=\cdots x_n=1$

$$\Rightarrow(x)^n(x)=x.x\ (mod\ n)$$
$$\Rightarrow x^{n-1}(x)=x\ (mod\ n)$$
$$\Rightarrow\ x^{\phi(n)+1}\equiv x(mod\ n)$$

A. Example

Apply Euler's Theorem to Solve the following Problem

a) $for\ any\ integer\ x,\ x^{13}\equiv x(mod\ 2370)$
b) $for\ any\ integer\ x,\ x^{37}\equiv x(mod\ 1729)$

Ans.

a) Euler's theorem show that forgcd$(x,n)=1$ has $x^{\phi(n)}\equiv 1(mod\ n)$,which is also relevant in this instance Fermat's little theorem $x^{p-1}\equiv 1(mod\ n)$.the exceptional case when n=p is prime
Let n=2730=2.3.5.7.13. Then, according to Fermat's little theorem,

$$x \equiv 1\ (mod\ 2)$$
$$x^2 \equiv 1\ (mod\ 3)$$
$$x^4 \equiv 1\ (mod\ 5)$$
$$x^6 \equiv 1\ (mod\ 7)$$
$$x^{12} \equiv 1\ (mod\ 13)$$

For x, the moduli are relatively prime. Any power on the left side will be congruent to 1 once more, and so on.

$$x^{12} \equiv 1\ (mod\ 2)$$
$$x^{12} \equiv 1\ (mod\ 3)$$
$$x^{12} \equiv 1\ (mod\ 5)$$
$$x^{12} \equiv 1\ (mod\ 7)$$
$$x^{12} \equiv 1\ (mod\ 13)$$

Again, for x the moduli are relatively prime. Multiply each of these by *x* to get $x^{13} \equiv x$ for all moduli and all integer *x* and all integer *x*. according to the Chinese remainder theorem

$$x^{13} \equiv x\ (mod\ 2.3.5.7.13)$$

For every integer *x*.

b) Let n=1729=7.13.19

Then, according to Fermat's little theorem,

$$x^6 \equiv 1\ (mod\ 7\ )$$
$$x^{12} \equiv 1\ (mod\ 13)$$
$$x^{18} \equiv 1\ (mod\ 19)$$

For x, the moduli are relatively prime. Any power on the left side will be congruent to 1 once more, and so on.

$$x^{36} \equiv 1\ (mod\ 7\ )$$
$$x^{36} \equiv 1\ (mod\ 13)$$
$$x^{36} \equiv 1\ (mod\ 19)$$

Multiply each of these by *x* to get $x^{37} \equiv x$ for all moduli and all integer *x* and all integer *x*. according to the Chinese remainder theorem

$$x^{37} \equiv x(mod\ 7.13.19\ )$$

For every integer *x*.

CASE 2: (n is not prime)

THEOREM. Assume that n is a positive natural number having prime factorization with$n = \prod_{i=0}^{k} p_i^{\gamma_i}$for $1 \le i \le k$. If x is an integer, then $x^{\phi(n)+1} \not\equiv x(mod\ n)$there exists at least one of$i,\ for\ which\ p_i^{\delta_i} | x\ and\ p_i^{\delta_i+1}\ Xx\ \ with\ 0 < \delta_i < \gamma_i$

PROOF Assume that for each $i, p_i^{\delta_i} | x\ and\ \ p_i^{\delta_i+1}\ Xx\ have$either$\delta_i = 0\ or\ \delta_i > \alpha_i$. We may suppose that for any$\delta_i > \gamma_i$for $1 \le i \le \gamma$ and $\delta_i = 0$ for$a + 1 \le i \le k$ since $x \equiv 0\left(mod\ p_i^{\gamma_i}\right)for1 \le i \le a$, we havegot

$$x^{\phi(n)+1} \equiv x\left(mod\ p_i^{\gamma_i}\right) \qquad (i)$$

For$1 \le i \le a$. We have $\gcd\left(x, p_i^{\gamma_i}\right) = 1$ for$a + 1 \le i \le k$, which implies $\gcd\left(x^m, p_i^{\gamma_i}\right) = 1$ for all natural integer m. By Euler's Theorem we also know$\phi(p_i^{\gamma_i}) | \phi(n)$ for $1 \le i \le k$so we have

$$x^{\phi(n)+1} = x^{\phi(n)} x = \left(x^{\frac{\phi(n)}{\phi(p_i^{\gamma_i})}}\right)^{\phi(p_i^{\gamma_i})} \qquad x \equiv 1.x$$
$$\equiv x\left(mod\ p_i^{\gamma_i}\right) \qquad (ii)$$

From the identity (i) and (ii), we have the following congruence system:

$$x^{\phi(n)+1} \equiv x\left(mod\ p_1^{\gamma_1}\right)$$
$$x^{\phi(n)+1} \equiv x\left(mod\ p_2^{\gamma_2}\right)$$
$$x^{\phi(n)+1} \equiv x\left(mod\ p_k^{\gamma_k}\right)$$

According to the Chinese Remainder Theorem,

Now we can conclude that $x^{\phi(n)+1} \equiv x(mod\ n)$.

To proceed it, we assume that for $i, p_i^{\delta_i} | x\ and\ \ p_i^{\delta_i+1}\ Xx\ \ with 0 < \delta_i < \gamma_i$.Thenwe obtain$p_i^{\gamma_i}\ Xx\ and\ p_i | x$; indicating that for $m > 1$,

$$x^m - x = x(x^{m-1} - 1) \not\equiv 0(mod\ p_i^{\gamma_i}\ )$$

Now we have that for any$m > 1, x^m \not\equiv x(mod\ n)$In particular, we have $x^{\phi(n)+1} \not\equiv x(mod\ n)$.

This finding directly results in the 2 corollaries listed below.

COROLLARY 1.Assume n is a natural number and let x is an integer. If $x^{\phi(n)+1} \not\equiv x(mod\ n)$, then$x^m \not\equiv x(mod\ n)$ for every$m > 1$.

COROLLARY 2 Assume n is a natural number. If and only if n is that the product of distinct primes then $x^{\phi(n)+1} \equiv x\left(mod\ p_k^{\gamma_k}\right)$ for any integer x.

B. Example

Apply Euler's Theorem to Solve the Following Problem

- $\boldsymbol{for\ any\ odd\ \ integer\ x,\ x^{33} \equiv x(mod\ 4080)}$

Ans.

Euler's theorem show that forgcd$(x, n) = 1$has $x^{\phi(n)} \equiv 1(mod\ n)$,which is also relevant in this instance Fermat's little theorem $x^{p-1} \equiv 1(mod\ n\ )$.the exceptional case when n is not prime.

Let n=1729=3.5.16.17

Then, according to Fermat's little theorem

$$x^2 \equiv 1\ (mod\ 3)$$
$$x^4 \equiv 1\ (mod\ 5)$$
$$x^8 \equiv 1\ (mod\ 16)$$
$$x^{16} \equiv 1\ (mod\ 17)$$

For x, the moduli are relatively prime. Any power on the left side will be congruent to 1 once more, and so on.

$$x^{32} \equiv 1\ (mod\ 3)$$
$$x^{32} \equiv 1\ (mod\ 5)$$
$$x^{32} \equiv 1\ (mod\ 16)$$
$$x^{32} \equiv 1\ (mod\ 17)$$

Again, for x the moduli are relatively prime. Multiply each of these by x to get

$$x^{33} \equiv x\ (mod\ 3)$$
$$x^{33} \equiv x\ (mod\ 5)$$
$$x^{33} \equiv x\ (mod\ 16)$$
$$x^{33} \equiv x\ (mod\ 17)$$

The first, second, and fourth congruence hold for all integer x. multiplying by x also makes the congruence hold for all integers x.The third holds for all integers relatively prime to 16 that is all odd integers. According to the Chinese remainder theorem

$$x^{33} \equiv x \ (mod\ 3.5.16.17)$$

For every integer x.

III. CONCLUSION

Euler's generalized Fermat's little theorem is a fundamental theorem in elementary number theory that assist in the calculation of powers of integers modulo prime numbers. It is a specific instance of Euler's theorem and is useful in elementary number theory applications such as primality checking and public-key cryptography.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

ACKNOWLEDGMENT

This research is supported and funded by C.V Raman Global University, Bhubaneswar, Odisha, India.

REFERENCES

[1] Niven, Zuckerman and Montgomery 1991, An Introduction to the Theory of Numbers, 4th edition (New York: Wiley).
[2] S.P Behera and A.C Panda, Nature Of Diophantine Equation 4x +12y= z2, International Journal of Innovative Research in Computer Science and Technology (IJIRCST), Vol.09 (6) (2021), 11-12.
[3] Diamond F, Shurman J. A first course in modular forms. Springer; 2005.
[4] N. Freitas and S. Siksek, The asymptotic Fermat's last theorem for five-sixths of real quadratic fields, Compos. Math.Vol18 (8) (2015) 1395–1415
[5] G. Turcas, On Fermat's equation over some quadratic imaginary number fields, Res. Number Theory 4 (2018) 24
[6] G. Turcas, On Fermat's equation over some quadratic imaginary number fields, Res. Number Theory 4 (2018) 24

ABOUT THE AUTHORS

Dr. Siva Prasad Behera is an Assistant Professor of Mathematics at C.V. Raman Global University, Bhubaneswar, Odisha. His main area of research includes Design and Analysis of Algorithms, Graph theory, Theory of Computations & Algebraic Number Theory.

Dr. Jitendra Kumar Pati is the Associate Professor in Department of Mathematics, C V Raman Global University, Bhubaneswar, Odisha. He has 20 years teaching experience. His research area includes Oscillatory and non-oscillatory behaviour of differential equations, Multi objective optimization, and Statistical analysis through logistic and multivariate regression models. He has published 15 papers in national and international journals.

Saroj Kumar patra is a M.sc Scholar in Applied Mathematics And computing, In C.V Raman Global University, Bhubaneswar, Odisha .He is currently working as a project scholar under the guidance of Dr. Siva Prasad Behera He has received B.sc degree in 2020 under Utkal university. His research interest in number theory

Prasanta Kumar Raut is a Research Scholar in Mathematics in C.V Raman GlobalUniversity,Bhubaneswar,odisha752054.He is currently working as a Project scholar under the guidance of Dr.Siva Prasad Behera.He has received M.sc degree in 2020 under C.V Raman Global university. His research area is Graph theory