OPPOSITE OF EULER'S THEOREM

By Shazly Abdullah

ABSTRACT

the work of José María Grau and Antonio M. Oller-marcén if $C_n(b) = nb^n + 1$ then $n^{b^n} \equiv (-1)^b (mod\, C_n(b))$ has been generalized to if $m = u(ut)^\beta + 1$ and $\phi(m) = \eta k$ where $\phi(m)$ is Eulere function then $(uv^{\beta-\eta} t^\beta)^k \equiv (-1)^k (mod\, m)$. Two proofs are presented to prove the generalization. The first is based on the binomial theorem and elementary algebra, and the second is based on the difference theorem and properties of congruence in particular.

1.INTRODUCTION

Historically the notion of congruence was first introduced and used systematicalIy in Gauss' Disquisitiones Arithmeticae. The notion of congruence is a wonderful example of the usefulness of employing the" right" discussion of congruences see Shafarevich [9]; shows how the theory of congruences is useful in determining whether equations can be solved in integers also see Davenport[22] H. Rosen[164] J. Tattersall[92] Among the questions that naturally emerged in congruence, how do we find solutions of congruence $a^n \equiv \pm(mod\, m\,)$ Is there an infinite number of solutions, if any, what are the properties of those solutions. in 1610 Fermat wrote in a letter to Frenicle, that whenever p is prime p divides $a^{p-1} - 1$ for all integers a not divisible p, a result now known as Fremat’s little theorem, As equivalent formulation is the assertion that p divides $a^p - a$ for all integers a, whenever p is prime . the question naturally arose as to whether the prime are the only integer exceeding that satisfy this criterion , but Carmichael pointed out in 1910 that 561=17×11×3 divides $a^{560} - 1$ Now we know that there is an infinite number of this kind of number that achieves the solution been He studied William Robert Alford, Andrew Granville, Carl Pomerance this kind of number. Euler proved and generalized the result to what is known as Euler's theorem. In 2011, José María Grau and Antonio M. Oller-marcén proved the following result: If $C_n = nb^n + 1$ is a generalized cullen number, then $n^{b^n} \equiv (-1)^b (mod\, C_n(b))$ also explained the result. A strong test for choline numbers, as it contains very few false verbs and has a lower computational cost

. The main objective of the paper in particular is to find solutions of congruence $a^n \equiv \pm(mod\, m\,)$ where $m = ux^k + 1$ and $a < m$ and to determine the properties of those solutions. More precisely, we are looking for the values of a, n that achieve the solution of congruence.

2. BASIC RESULTS

In this section in particular we study the test of generalized Collin numbers and answer some questions about the test, why are there wrong verbs in the test, is there a relationship between the test and Fermat's Litter Theorem We will answer these questions after proving LEMMA (1) in two ways: Method One It depends on the properties and rules of congruence, and the second method depends on the binomial theorem. The result shows us the deep relationship between the test and Fermat's Lesser Theorem.

LEMMA 1. If $h = ad + 1$ and $a\ d\ n\ \in \mathbb{N}$ then

$$a^n \equiv (-1)^n (mod\ h) \Leftrightarrow d^n \equiv 1 (mod\ h)$$

Proof 1. if $h = ad + 1$ *we have*

$$(ad)^n \equiv (-1)^n (mod\ \ h) \qquad (\ \ )$$

See proof in Kenneth H. Rosen [96, 94] to discuss this topic and the properties of congruence in detail . Now from ( ) we find that

$$a^n \times d^n \equiv 1 \times (-1)^n \big(mod\ C_m(k)\big) \qquad (\ \ )$$

Congruence multiplication properties To learn more about multiplication and addition properties for a related discussion see Kenneth H. Rosen [94,93] and Kenneth Ireland Michael Rosen [30,29] from ( ) we have that

$$a^n \equiv (-1)^n (mod\ h) \Leftrightarrow d^n \equiv 1\big(mod\ C_m(k)\big)$$

∎

Proof 2. If $m = ad + 1$ From binomial theorem we have

$$(1 - m)^n - \big(1 + (a - 1)\big)^n = \sum_{j=1}^{n} (-1)^j \binom{n}{j} \big((-ad + 1)^j - (-a + 1)^j\big)$$

Then

$$(-ad)^n - a^n = \sum_{j=1}^{n} (-1)^j \binom{n}{j} \big(m^{n-j} - (-a + 1)^{n-j}\big) \qquad (\ \ )$$

From the difference of tow nth power theorem we have

$$\mathrm{m}^n - (-a + 1)^n = (ad + a) \sum_{k=1}^{n} \mathrm{m}^{k-1} (-a + 1)^{j-k} \qquad (\ \ )$$

Substituting equation ( ) into equation ( ) we get

$$\begin{aligned}(-ad)^n - \mathrm{a}^n &= \sum_{j=1}^{n} (-1)^j \binom{n}{j} \big(\mathrm{m}^j - (-a + 1)^j\big) \\ &= \sum_{j=1}^{n} (-1)^j \binom{n}{j} \left((ad + a) \sum_{k=1}^{j} \mathrm{m}^{k-1} (-a + 1)^{j-k} \right) \\ &= (ad + a) \sum_{j=1}^{n} \sum_{k=1}^{j} (-1)^{j+1} \binom{n}{j} m^{k-1} (-a + 1)^{j-k}\end{aligned}$$

$$= -(ad+a)\sum_{k=1}^{n}\binom{n}{k}(-a+1)^{k-1} + (ad+a)\sum_{j=2}^{n}\sum_{k=j}^{n}\binom{n}{k}(-1)^{j}m^{j-1}(-a+1)^{k-j}$$

$$= \frac{(ad+a)}{a-1}(a^{n}-1) + (ad+a)\sum_{j=2}^{n}\sum_{k=j}^{n}\binom{n}{k}(-1)^{j}m^{j-1}(a-1)^{k-j}$$

Therefore

$$a^{n-1}((-d)^{n}-1) = \frac{(d+1)}{a-1}(a^{n}-1) + (d+1)\sum_{j=2}^{n}\sum_{k=j}^{n}\binom{n}{j}(-1)^{j}\mathrm{m}^{j-1}(-a+1)^{k-j}$$

Subtracting $\frac{(d+1)}{a-1}(a^{n}-1)$ from both sides of the equation we get

$$a^{n-1}((-d)^{n}-1) - \frac{(d+1)}{a-1}(a^{n}-1)$$

$$= (d-1)\sum_{j=2}^{n}m^{j-1}\left(\sum_{k=j}^{n}\binom{n}{j}(-1)^{j}(-a+1)^{k-j}\right) \qquad (\quad)$$

Note the right-hand side of equation (   ) is divisible by m for all values of n

$$(d-1)\sum_{j=2}^{n}m^{j-1}\left(\sum_{k=j}^{n}\binom{n}{j}(-1)^{j}(-a+1)^{k-j}\right) \equiv 0(mod\, m) \quad all \;\; n = 1,2,\ldots\ldots \; (\quad)$$

From equation (   ) and (   ) then we have

$$a^{n-1}((-d)^{n} \equiv 1)(mod\, m) \Leftrightarrow \frac{(d+1)}{a-1}(a^{n} \equiv 1)(mod\, m)$$

$m = ad + 1$ so g.c.d$\left(\frac{(d+1)}{a-1}, m\right)$ =g.c.d$\left(a^{n-1}, m\right) = 1$ then

$$d^{n} \equiv (-1)^{n}(mod\, m) \Leftrightarrow a^{n} \equiv 1(mod\, m)$$

Remark. Proof 1 depends on the properties of congruence in multiplication and division Proof 2 is more complicated than the other and depends on the binomial theorem. We note that equation (┤) has been replaced by (┤) , then arrange the new terms and then deduce the congruence from the equation. The arrangement process is the most important step in proof 2

LEMMA 2 . if $\mathcal{D}_{\mathrm{V}} = \left\{\mathrm{k}: \frac{\phi(h)}{k}, 2 \le \mathrm{k} \le \mathrm{m},\; h = \mathrm{u}x^{m} + 1\,,\; h \in \mathbb{N} - \{0,1\}\right\}$ where $\forall a \in \mathcal{D}_{\mathrm{v}}$ we have

$$(ux^{m-a})^{\frac{\phi(h)}{a}} \equiv (-1)^{\frac{\phi(h)}{a}}(mod\, h)$$

Proof. Let $a = k^{a_1}$ *and* $n = \frac{\phi(m)}{a_1}$ and $d = ux^{m-a_1}$ in **lemma 1** then $h = ux^{m} + 1$ where $a_1 \in \mathcal{D}_{\mathrm{v}}$ and $\mathcal{D}_{\mathrm{v}} = \left\{\mathrm{k}: \frac{\phi(h)}{k}, 2 \le \mathrm{k} \le \mathrm{m},\; h = \mathrm{m}x^{m} + 1\,,\; h \in \mathbb{N} - \{0,1\}\right\}$ then we have

$$(uk^{m-a_1})^{\frac{\phi(h)}{a_1}} \equiv (-1)^{\frac{\phi(h)}{a_1}}(mod\, h) \Leftrightarrow (k^{a_1})^{\frac{\phi(h)}{a_1}} \equiv 1(mod\, h) = k^{\phi(h)} \equiv 1(mod\, h)$$

Let x,u∈ ℕ Substituted $a = k^{a_1}$ $n = \frac{\phi(h)}{a_1}$ $d = uk^{m-a_1}$ into the lemma 1 $a_1 \in \mathcal{D}_{\mathrm{v}}$ where when we congruence $(x^{a_1})^{\frac{\phi(h)}{a_1}} \equiv 1(mod\, h)$ we get $x^{\phi(h)} \equiv 1(mod\, h)$and from Euler's theorem then

$$(ux^{m-a_1})^{\frac{\phi(h)}{a_1}} \equiv (-1)^{\frac{\phi(h)}{a_1}}(mod\, h)$$

If $a = x^{a_2}$ *and* $n = \frac{\phi(m)}{a_2}$ $d = ux^{m-a_2}$ in **lemma 1** where $a_2 \in \mathcal{D}_{\mathrm{v}}$ and $a_2 \neq a_1$ then we have

$$(ux^{m-a_2})^{\frac{\phi(h)}{a_2}} \equiv (-1)^{\frac{\phi(h)}{a_2}}(mod\, h) \Leftrightarrow (x^{a_2})^{\frac{\phi(h)}{a_2}} \equiv 1(mod\, h) = x^{\phi(h)} \equiv 1(mod\, h)$$

a_2 were chosen from group$a_2 \in \mathcal{D}_{\mathrm{V}}$,where$a_2 \neq a_1$ according to the group's conditions, now substituted $a = k^{a_2}$ in LEMMA 1 then $(x^{a_2})^{\frac{\phi(h)}{a_2}} \equiv 1(mod\, h) = x^{\phi(h)} \equiv 1(mod\, h)$ from Euler's theorem then we have that

$$\begin{array}{ll}
(ux^{m-a_1})^{\frac{\phi(h)}{a_1}} \equiv (-1)^{\frac{\phi(h)}{a_1}}(mod\, h) & , a_1 \in D_V \\
(uk^{m-a_2})^{\frac{\phi(h)}{a_2}} \equiv (-1)^{\frac{\phi(h)}{a_2}}(mod\, h) & , a_2 \in \mathcal{D}_{\mathrm{V}} \\
(uk^{m-a_3})^{\frac{\phi(h)}{a_3}} \equiv (-1)^{\frac{\phi(h)}{a_3}}(mod\, h) & , a_3 \in \mathcal{D}_{\mathrm{V}} \\
(uk^{m-a_4})^{\frac{\phi(h)}{a_4}} \equiv (-1)^{\frac{\phi(h)}{a_4}}(mod\, h) & , a_4 \in \mathcal{D}_{\mathrm{V}} \\
\ldots\ldots\ldots\ldots\ldots.\ldots\ldots\ldots & \\
\ldots\ldots\ldots\ldots\ldots.\ldots.\ldots\ldots\ldots & \\
\ldots\ldots\ldots\ldots\ldots..\ldots\ldots.. & \\
(uk^{m-a_i})^{\frac{\phi(h)}{a_i}} \equiv (-1)^{\frac{\phi(h)}{a_i}}(mod\, h) & , a_i \in \mathcal{D}_{\mathrm{V}} \ , i < \mathrm{V} \\
\ldots\ldots\ldots\ldots\ldots\ldots.\ldots\ldots\ldots.. & \\
\ldots\ldots\ldots\ldots\ldots\ldots..\ldots\ldots\ldots\ldots.. & \\
\ldots\ldots\ldots\ldots\ldots..\ldots\ldots\ldots\ldots\ldots\ldots & \\
(uk^{m-a_{(\tau(h)\sim m)}})^{\frac{\phi(h)}{a_{(\tau(h)\sim m)}}} \equiv (-1)^{\frac{\phi(h)}{a_{(\tau(h)\sim m)}}}(mod\, h) & , a_V \in \mathcal{D}_{\mathrm{V}}
\end{array}$$

Then

$$(uk^{m-a})^{\frac{\phi(h)}{a}} \equiv (-1)^{\frac{\phi(h)}{a}}(mod\, h) \quad all\ a \in \mathcal{D}_{\mathrm{V}}$$

Then $h = mk^m + 1 = C_n(k)$ from

$$m^{k^m} \equiv (-1)^{k^m}(mod\, h) \Leftrightarrow k^{C_n(k)-1} \equiv 1(modC_n(k))$$

3. GENERALIZING EULER'S THEOREM

In this section, we generalize the test of Collin's generalized numbers. The components of the proof are result 6, which shows the equivalence relationship between the congruents, Euler's theorem and Fermat's Lesser Theorem. It is also worth noting that we will use the same test to prove the generalization.

THEOREM 1. If $h = ux^m + 1$ and $\mathcal{G}_{\tau(h)-1} = \left\{a\colon \frac{h-1}{a} \ , h = ux^m + 1\,, h \in \mathbb{N}\right\}$ and $\phi(h)\ is\ Euler\ function$ where $\mathcal{D}_V = \left\{k\colon \frac{\phi(h)}{k}\ , \ 2 \leq k \leq m, \quad h = ux^m + 1 \ , h \in \mathbb{N}\right\}$ then

$$\left\{\begin{array}{l}
\theta^{\ell} \equiv (-1)^{\ell}(mod\, h) \ \ if \ \ \theta^{\ell} \in \psi_{\mathcal{H}_E} \\
\qquad\qquad\qquad\qquad where \qquad \psi_{\mathcal{H}_E} = \bigcup_{q=1}^{\tau(h)-1} \mathcal{H}_{E_q} \\
\mathcal{H}_{E_q} = \left\{{\theta_q}^{\ell_1}, {\theta_q}^{\ell_2}, {\theta_q}^{\ell_3}, {\theta_q}^{\ell_4} \ldots\ldots..{\theta_q}^{\ell_V}\right\} \\
if \ \ \theta_q \in \mathcal{G}_{\tau(h)-1} \ \ q = 1,2,3 \ldots\ldots \tau(h) - 1 \ \ and \ \ \ell_j \in \mathcal{D}_{\mathrm{V}} \ \ j = 1,2 \ldots..V
\end{array}\right.$$

Proof.Let $h = kx^m + 1\, where\;\; x = \prod_{j=1}^{n} E_j \quad \mathcal{G}_W = \left\{a :\ \frac{ux}{a}\ , h = ux^m + 1\ , h \in \mathbb{N}\right\}$ $and\ in\ lemma\ 1\ let\ a = {E_1}^q\ and\ E_1 \in \mathcal{G}_W\ where\;\; q \in \mathcal{D}_V\;\; j = 1,2,3 \ldots \ldots$ V we have

$$\left(\frac{h-1}{{E_1}^a}\right)^{\frac{\phi(h)}{a}} \equiv (-1)^{\frac{\phi(h)}{a}} (mod\ h) \Leftrightarrow \left({E_1}^a\right)^{\frac{\phi(m)}{a}} \equiv 1 (mpd\ h)$$

$$\left(k{E_1}^{m-a}\left(\prod_{j=2}^{n} E_j\right)^{m}\right)^{\frac{\phi(h)}{a}} \equiv (-1)^{\frac{\phi(h)}{a}} (mod\ h)$$

If $u = k\left(\prod_{j=2}^{n} E_j\right)^m$ we have

$$(u{E_1}^{m-a})^{\frac{\phi(h)}{a}} \equiv (-1)^{\frac{\phi(h)}{a}} (mod\ h)$$

Let $\theta_1 = (u{E_1}^{m-a_j})$ and $\ell_j = \frac{\phi(h)}{a_j}\ so\ {\theta_1}^{\ell_j} = (u{E_1}^{m-a_j})^{\frac{\phi(h)}{a_j}}$ where

$$\mathcal{H}_{E_1} = \left\{{\theta_1}^{\ell_1}, {\theta_1}^{\ell_2}, {\theta_1}^{\ell_3}, {\theta_1}^{\ell_4} \ldots \ldots \ldots . {\theta_1}^{\ell_V}\right\}$$

From lemma 1 we get

$$\left(u{E_1}^{m-a}\right)^{\frac{\phi(h)}{a}} \equiv (-1)^{\frac{\phi(h)}{a}} (mod\ h)\quad all\ a \in \mathcal{D}_V$$

Then

$${\theta_1}^{\ell} \equiv (-1)^{\ell} (mod\ m)\;\; where \quad \forall\, {\theta_1}^{\ell}\ \in \mathcal{H}_{E_1}$$

We note in the equation (   ) a proof of all the elements of the set β_V, and this means that we have worked to determine the values of the exponent n to congruence $a^n \equiv 1 (mod\ m)$ that which achieves the solution $n = \frac{\phi(m)}{\lambda_1}, \frac{\phi(m)}{\lambda_2}, \frac{\phi(m)}{\lambda_3} \ldots \ldots . . \frac{\phi(m)}{\lambda_{\beta \sim \tau(\phi(m))}}$, and it is known about the base

Equals $a = \omega{\eta_1}^{\beta-\lambda_j}v^{\beta}$ We notice values that $\omega\eta_1 v$ have not changed By definition $x = \eta_1 v$. We just change the values of the exponent $\beta - \lambda_j\beta$ by choosing all the elements of the set $\forall\lambda \in\ \beta_{\beta\sim\tau(\phi(m))}$

Let $a \in \mathcal{D}_{\mathrm{V}}$ and $\frac{x}{E_2}$ where $a = {E_2}^a$ we get

$$\mathcal{H}_{E_2} = \left\{{\theta_2}^{\ell_1}, {\theta_2}^{\ell_2}, {\theta_2}^{\ell_3}, {\theta_2}^{\ell_4} \ldots \ldots \ldots \ldots . {\theta_2}^{\ell_{\mathrm{V}}}\right\}$$

Then

$${\theta_2}^{\ell} \equiv (-1)^{\ell} (mod\ m)\, where \quad \forall\;\ {\theta_2}^{\ell}\ \in \mathcal{H}_{E_2}$$

Then let $\mathcal{H}_{E_1}, \mathcal{H}_{E_2}, \mathcal{H}_{E_3}, \mathcal{H}_{E_4} \ldots \ldots \ldots . \mathcal{H}_{E_{(\tau(x)-1)}}$ if

$$\psi_{\mathcal{H}_E} = \bigvee_{j=1}^{(\tau(x)-1)} \mathcal{H}_{E_j}$$

Then all $\forall\delta \in \psi_{\mathcal{H}_\eta}$ we have

$$\delta \equiv 1 (mod\ m)$$

Let $a = {p_1}^{q_2}$ and $n = \frac{\phi(m)}{q_2}$ we have

$$\left(p_1{}^{q_2}\right)^{t-1}\left(\left(\frac{m+1}{p_1{}^{q_2}}\right)^{\frac{\phi(m)}{q_2}}-1\right)=\mathrm{T}\left(\left(p_1{}^{q_2}\right)^{\frac{\phi(m)}{q_2}}-1\right)+\mathrm{mV}$$

Then

$$\left(p_1{}^{q_2}\right)^{t-1}\left(\left(\frac{m+1}{p_1{}^{q_2}}\right)^{\frac{\phi(m)}{q_2}}-1\right)=T\left(p_1{}^{\phi(m)}-1\right)+\mathrm{mV}$$

We note $n=\frac{\phi(m)}{q_2}$ we have

$$ord_m\left(p_1\right)=\phi(m)\ \ then\ \ ord_m\left(\frac{m+1}{p_1{}^{q_2}}\right)=\frac{\phi(m)}{q_2}$$

Then

$$ord_m\left(p_q\right)=\phi(m)\ \ then\ \ ord_m\left(\frac{m+1}{p_q{}^{q_f}}\right)=\frac{\phi(m)}{q_f}$$

where

$$\mathcal{Q}_n=\left[a:\ ,\ \ a=\lambda_1+\lambda_2\ldots+\lambda_n\ \ ,\lambda_1,\lambda_2,\ldots\lambda_n\in\beta_{\beta\Delta(\tau(\phi(m))-1)}\ \right]$$

Proof . All

From congruence theorem we find if $a^d\equiv 1(mod\ m)\ and\ a^k\equiv 1(mod\ m)$ we have $a^{d+k}\equiv 1(mod\ m)$ if $k\ \ d\ \ \in\beta_{\beta\Delta(\tau(\phi(m))-1)}\ or\ \mathcal{P}_{2\chi}$ let

$$\mathcal{Q}_n=\left[a:2\le a\le\phi(m)\ \ ,a=b+c\ \ ,b,c\in\beta_{\beta\Delta(\tau(\phi(m))-1)}\ or\ \mathcal{P}_{2\chi}\right]$$

We note from group of numbers $\mathcal{P}_{2\chi}\le\beta_{\beta\Delta(\tau(\phi(m))-1)}<\mathcal{Q}_n$

References

1. H. S. Rose . A Course in Number Theory " Oxford Science publications (1988).
2. K. M. Rose, Elementary Number Theory" 4th Edition Addison- Wesley (2000)

3. R. K. Guy , Unsolved Problems in Number Theory 3rd . ed Springer, (2004).
4. James J. Tattersall Elementary Number Theory in Nine Chapters Cambridge University Press 2005
5. Grau, José Maria and Oller-Marcén, Antonio M., "An ~O(log 2(N)) time primality test for generalized Cullen numbers," Math. Comp., 80:276 (2011) 2315--2323. (http://dx.doi.org/10.1090/S0025-5718-2011-02489-0) MR 2813363
6. Löh, Günter; Niebuhr, Wolfgang A new algorithm for constructing large Carmichael numbers. Math. Comp. 65 (1996), no. 214, 823–836.
7. Pinch, R. G. E. The Carmichael numbers up to 10^{15}. Math. Comp. 61 (1993), no. 203, 381–391.
8.

Student: Shazly Abdullah Faculty of mathematics sciences & statistics Al-neelain University Sudan Shazlyabdullah3@gmail.com