Chapter

On the Analytical Properties of Prime Numbers

Shazali Abdalla Fadul

Abstract

In this work we have studied the prime numbers in the model $P = am + 1, m, a > 1 \in \mathbb{N}$. and the number in the form $q = ma^m + bm + 1$ in particular, we provided tests for hem. This is considered a generalization of the work José María Grau and Antonio M. Oller-marcén prove that if $C_m(a) = ma^m + 1$ is a generalized Cullen number then $m^{a^m} \equiv (-1)^a (mod\ C_m(a))$. In a second paper published in 2014, they also presented a test for Broth's numbers in Form $kp^n + 1$ where $k < p^n$. These results are basically a generalization of the work of W. Bosma and H.C Williams who studied the cases, especially when $p = 2, 3$, as well as a generalization of the primitive MillerRabin test. In this study in particular, we presented a test for numbers in the form $ma^m + bm + 1$ in the form of a polynomial that highlights the properties of these numbers as well as a test for the Fermat and Mersinner numbers and $p = ab + 1\ a, b > 1 \in \mathbb{N}$ and $p = qa + 1$ where q *is prime odd* are special cases of the number $ma^m + bm + 1$ when b takes a specific value. For example, we proved if $p = qa + 1$ where q is odd prime and $a > 1 \in \mathbb{N}$ where $\pi_j = \frac{1}{q}\binom{q}{j}$ then $\sum_{j=1}^{q-2} \pi_j (-C_m(a))^{q-j-1}(q - a^m) \equiv \chi_{(m, q-a^m)}(mod\ p\ )$ Components of proof Binomial theorem Fermat's Litter Theorem Elementary algebra.

Keywords: broth numbers, Cullen number, polynomial, Fermat number, Mersinne numbers

1. Introduction

No algorithm that produces prime numbers in explicit forms, or rather, this goal was not reached, mathematicians resorted to an alternative method to discover prime numbers, which are primitive tests since Fermat's era or before, and this method proved its effectiveness to the extent that many prime numbers were discovered The Great Until. Euler studied Fermat's prime numbers and discovered some of them. Cullen, Broth and Mersinne also studied those numbers, as well as Pedro Berrizbeitia, Wieb Bosma and A. Schönhage. The results that we reached in this study are in the same way as those who followed the work of [1–3]. In a paper published on March 11, 2011 MO [3] prove the following result. $\boldsymbol{C_m(a)}$ is a prime where $\boldsymbol{C_m(a) = ma^m + 1}$ then

$m^{a^m} \equiv (-1)^a (mod\ C_m(a))$ And in a paper published on July 10, 4102 using the same ideas found in MO [2], they proved [3] the following result. Let $N = kp^n + 1$.

where is p is odd prime and $k < p^n$ Assume that $a \in \mathbb{Z}$ is a p-th power non-residue modulo N, then N is a prime if only if $\phi_p\left(a^{\frac{N-1}{p}}\right) \equiv 0(mod\ N)$. The numbers in form $C_m(a) = ma^m + 1$ are called Cullen numbers, first studied by Cullen in 1905. And the numbers in the form of $kp^n + 1$ are called the Broth numbers and we call the number primes the form $M_P = 2^P - 1$ mersenne number discovered in 2005 by Martin nowak the largest prime number of Mersenne $M_{25964951}$ and 42 in the list. We know about Mersenne's number if M_p it is not prime then there is a prime number $q = 2pr + 1$ where M_p/q example M_{11} of a non-prime. Also there is a relationship between Mersenne prime and the perfect numbers. And number in form $F_n = 2^{2^n} + 1$ are called Fermat numbers were first studied by Pierre de Fermat, The importance of these numbers lies in providing the large prime numbers of the known. All the large prime numbers are in the form $ma^n + b$ or $a^n + b$, for example, in 2021, $2525532.73^{2525532} + 1$ was discovered the largest prime number defined by Tom Greer. There is a program in the Internet called [Prime Grid] The goal of discovering this is a kind of numbers See [$https:\ \ primegrid.com$] Researchers use several techniques in the study such as preliminary tests and high-precision computers. Prove Broth if $N = k2^n + 1$ where K is odd and $k < 2^n$ if $a^{\frac{N-1}{2}} \equiv -1(mod\ N)$ same $a \in \mathbb{Z}$ then N is a prime. The next important step was made in 1914 by Pocklington his result is the first generalization of Proth's theorem suitable for numbers of the form prove Pocklington if $N = Kp^n + 1$ where K is odd and $k < p^n$ if for same $a \in \mathbb{Z}$ $a^{N-1} \equiv -1(mod\ N)$ $and\ g.c.d\left(a^{\frac{N-1}{p}} - 1, p\right)$ then N is prime. There are many works that discuss Broth's theorem and numbers. Case $p = 3$ studied by W. Bosma [4] and A. Guthmann [5] Also, for a discussion on the Broth numbers, see H.C Williams [6, 7] P. Berrizbeitia [8, 9].

The purpose of this work is to study the numbers in model $ma^m + bm + 1$ and $p = ba + 1$ where $a, b > 1 \in \mathbb{Z}$ and $p = aq + 1, a, q \in \mathbb{N}$ where q is an odd prime number, In addition, tests for Fermat and Mersenne numbers are presented and the study of the relationship between two prime numbers and a polynomial with finite properties. From the results we obtained we proved, for example, if p and q are prime numbers, $p = qa + 1$ where $q, a > 1 \in \mathbb{N}$ and where $C_m(a) = ma^m + 1$ and $\pi_j = \frac{1}{q}\binom{q}{j}$ then

$$\sum_{j=1}^{q-2} \pi_j (-C_m(a))^{q-j-1}(q - a^m) \equiv \chi_{(m, q-a^m)}(mod\ p) \qquad (1)$$

Our approach to the proof differs from the one in [2, 3]. We explicitly relied on the binomial theorem, elementary algebra, and Fermat's litter theorem. A deductive method of analysis using basic operations in elementary algebra.

2. Proof of the theorem 1

In this section, we prove theorem 1. Components of the proof Elementary algebra basic operations such as subtraction from both sides and extraction of the common factor with the binomial theorem form the foundations of the proof. Theorem 1 is an expression of a polynomial that shows the properties of numbers in the form $p = ma^m + bm + 1$,

$a, m, b > 1 \in \mathbb{N}$, so it can be used as a test to reveal the prime number in the form $ma^m + bm + 1$. In addition to that, it is used to prove the results in the next section where it plays an essential role in the proofs.

THEOREM 1 if M is a prime where $\mathcal{M} = ma^m + bm + 1$ *and* $a, m > 1 \in \mathbb{N}, b \neq 0 \in \mathbb{Z}$ then

$$\begin{cases} \eta_{(\lambda)} \equiv \chi_{(x,y)} (mod\ \mathcal{M}) & if\ \mathcal{M}\ and\ \lambda\ is\ a\ prime\ where \\ \\ \eta_{(\lambda)} \equiv \chi_{(\lambda,x,y)} (mod\ \mathcal{M}) & if\ \mathcal{M}\ is\ a\ prime \end{cases} \tag{2}$$

Proof. let $\mathcal{M} = ma^m + \delta\ where\ m, a,$ n $> 1 \in \mathbb{N}$ and $\delta = bm + 1$ where $b \in \mathbb{Z}$ according to the binomial theorem, we find that

$$(\mathcal{M} + (-\delta))^n - m^n = (ma^m)^n - m^n = \sum_{j=0}^{n-1} \binom{n}{j} \mathcal{M}^{n-j} (-\delta)^j + (-\delta)^n - m^n \tag{3}$$

Then

$$m^n (a^{mn} - 1) - ((-bm - 1)^n - m^n) = \sum_{j=1}^{n-1} \binom{n}{j} \mathcal{M}^{n-j} (-bm - 1)^j \tag{4}$$

Note that

$$\sum_{j=0}^{n-1} \binom{n}{j} \mathcal{M}^{n-j} (-bm - 1)^j \equiv 0 (mod\ \mathcal{M}) \tag{5}$$

Then from (4) and (5) we have that

$$a^{nm} - 1 - ((-bm - 1)^n - m^n) \equiv 0 (mod\ \mathcal{M}) \tag{6}$$

Now we conclude that from Eq. (6)

$$a^{nm} \equiv 1 (mod\ \mathcal{M})\ if\ and\ only\ if\ (-bm - 1)^n \equiv m^n (mod\ \mathcal{M}) \tag{7}$$

Suppose that $n = \frac{\mathcal{M}-1}{m}$ and $\mathcal{M}$ is a prime so

$$a^{\mathcal{M}-1} \equiv 1 (mod\ \mathcal{M})\ if\ and\ only\ if\ (-bm - 1)^{\frac{\mathcal{M}-1}{m}} \equiv m^{\frac{\mathcal{M}-1}{m}} (mod\ \mathcal{M}) \tag{8}$$

From the assumption $\mathcal{M}$ is a prime from Fermat's litter theorem see [Kenneth H. Rosen 2 pp. 161] we have that if $\mathcal{M}$ *is a prime* then $a^{\mathcal{M}-1} \equiv 1\ (mod \mathcal{M}\ )$ where $a > 1$. This means if $\mathcal{M}$ is a prime number, then from (8) we find that

$$(-bm-1)^{\frac{\mathcal{M}-1}{m}} \equiv m^{\frac{\mathcal{M}-1}{m}}(mod\ \mathcal{M}) \tag{9}$$

Then

$$(bm+1)^{\frac{\mathcal{M}-1}{m}} \equiv (-m)^{\frac{\mathcal{M}-1}{m}}(mod\ \mathcal{M}) \tag{10}$$

Let be $\lambda = \frac{\mathcal{M}-1}{m}$ $\lambda = a^m + b$ then from binomial theorem we have that

$$\begin{aligned}(bm+1)^\lambda - (-m)^\lambda &= \sum_{j=0}^{\lambda}\binom{\lambda}{j}(bm)^{\lambda-1} - (-m)^\lambda \\ &= (bm)^\lambda - (-m)^\lambda + \sum_{j=1}^{\lambda-1}\binom{\lambda}{j}(bm)^{\lambda-1} + 1\end{aligned} \tag{11}$$

$\mathcal{M} = ma^m + bm + 1$ then $\lambda = \frac{\mathcal{M}-1}{m} = a^m + b$ According to the binomial theorem, if λ is a prime number, then $\binom{\lambda}{j} \equiv 0(mod\ \mathcal{M})$ means $\binom{\lambda}{j}$ is divisible by λ for every

$2\ \leq \lambda \leq \lambda - 1$. So suppose λ is a prime number and $\pi_j = \frac{1}{\lambda}\binom{\lambda}{j}$ follows from that $\binom{\lambda}{j}(bm) = \pi_j b(\mathcal{M}-1)$. so from (11) we have that

$$\begin{aligned}(bm+1)^\lambda - (-m)^\lambda &= (bm)^\lambda - (-m)^\lambda + 1 \\ &\quad + \sum_{j=1}^{\lambda-1}\pi_j b^{\lambda-j} m^{\lambda-j-1}(\mathcal{M}-1) \\ &= (bm)^\lambda - (-m)^\lambda + 1 + \left(\sum_{j=1}^{\lambda-1}\pi_j b^{\lambda-j} m^{\lambda-j-1}\right)\mathcal{M} \\ &\quad - \sum_{j}^{\lambda-1}\pi_j b^{\lambda-j} m^{\lambda-j-1}\end{aligned} \tag{12}$$

From Eq. (10) $(bm+1)^\lambda \equiv (-m)^\lambda(mod\ \mathcal{M})$. and Notice the Eq. (12) on the right-hand side consisting of two terms the first multiplied by $\mathcal{M}$ and the second empty of $\mathcal{M}$. Then we have that

$$\left(\sum_{j=1}^{\lambda-2}\pi_j b^{\lambda-j} m^{\lambda-j-1}\right)\mathcal{M} \equiv 0(mod\ \mathcal{M}) \tag{13}$$

And

$$(bm)^\lambda - (-m)^\lambda - \sum_{j=1}^{\lambda-2}\pi_j b^{\lambda-j} m^{\lambda-j-1} - b + 1 \equiv 0(mod\ \mathcal{M}) \tag{14}$$

Then

$$\sum_{j=1}^{\lambda-2} \pi_j b^{\lambda-j} m^{\lambda-j-1} \equiv (bm)^\lambda - (-m)^\lambda - b + 1 (mod\ \mathcal{M}) \tag{15}$$

Let be $\eta_{(\lambda)}(x,y) = \sum_{j=1}^{\lambda-2} \pi_j x^{\lambda-j} y^{\lambda-j-1}$ and $\chi_{(x,y)} = (bm)^\lambda - (-m)^\lambda - b + 1$ So we have that

$$\eta_{(\lambda)}(x,y) \equiv \chi_{(x,y)} (mod\ \mathcal{M}) \tag{16}$$

This is the first case of proof when λ is a prime. The proof of the second case is similar to the case of the first and there is no fundamental difference, according to the binomial theorem let be $\lambda > 2 \in \mathbb{N}$ then from (12) we have

$$\begin{aligned} \lambda\left((bm+1)^\lambda - (-m)^\lambda\right) &= \lambda\left((bm)^\lambda - (-m)^\lambda\right) + \lambda + \sum_{j=1}^{\lambda-1} \binom{\lambda}{j} b^{\lambda-j} m^{\lambda-j-1} (\mathcal{M}-1) \\ &= \lambda\left((bm)^\lambda - (-m)^\lambda\right) + \lambda + \left(\sum_{j=1}^{\lambda-1} \binom{\lambda}{j} b^{\lambda-j} m^{\lambda-j-1}\right)\mathcal{M} \\ &\quad - \sum_{j=1}^{\lambda-2} \binom{\lambda}{j} b^{\lambda-j} m^{\lambda-j-1} - \lambda b \end{aligned} \tag{17}$$

Note that

$$\left(\sum_{j=1}^{\lambda-1} \binom{\lambda}{j} b^{\lambda-j} m^{\lambda-j-1}\right)\mathcal{M} \equiv (mod\ \mathcal{M}) \tag{18}$$

And from (10) we have that

$$\lambda\left((bm+1)^\lambda - (-m)^\lambda\right) \equiv 0 (mod\ \mathcal{M}) \tag{19}$$

Then

$$\sum_{j=1}^{\lambda-2} \binom{\lambda}{j} b^{\lambda-j} m^{\lambda-j-1} \equiv \lambda(bm)^\lambda - \lambda(-m)^\lambda + \lambda - b\lambda (mod\ \mathcal{M}\ ) \tag{20}$$

Let be $\eta_{(\lambda)}(x,y) = \sum_{j=1}^{\lambda-2} \binom{\lambda}{j} x^{\lambda-j} y^{\lambda-j-1}$ and $\chi_{(\lambda,y,x)} = \lambda(bm)^\lambda - \lambda(-m)^\lambda + \lambda - \lambda b$ so we have

$$\eta_{(\lambda)}(x,y) \equiv \chi_{(\lambda,x,y)} (mod\ \mathcal{M}) \tag{21}$$

Then

$$\begin{cases} \eta_{(\lambda)}(x,y) \equiv \chi_{(y,x)} (mod\ \mathcal{M}) & if\ \lambda\ and\ \mathcal{M}\ is\ aprime \\ \eta_{(\lambda)}(x,y) \equiv \chi_{(\lambda,y,x)} (mod\ \mathcal{M}) & if\ \mathcal{M}\ is\ a\ prime \end{cases} \tag{22}$$

REMARK 1: We note that the proof has little complexity, as we explicitly relied on the binomial theorem and elementary algebra to obtain Eq. (12). After that, Fermat's Litter Theorem was used, which is a theorem dating back to the year 1610.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 divide $a^p - a$ 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 = 11 × 17 × 3 divides a $a^{560} \equiv 1(mod\ 561)$ now. A composite integer which satisfies $a^{n-1} \equiv 1(mod\ n)$ for all positive integers a with g.c.d(a, n) = 1 is called a Carmichael number. For a related discussion see Kenneth H. Rose page (55). This means that Theorem 1 is not a definitive test, but it fails at the numbers Carmichael, but on the one hand we find that it is more general than those [2, 10] because of the variables m, a, b in the number $ma^m + bm + 1$. And we will explain this by proving results for Mersenne and Fermat numbers, which are special cases when the variable b takes a certain value.

THEOREM 2. *if* $\lambda = a^m + (-1)^\sigma$ and $q = ma^m + (-1)^\sigma m + 1$ where q is a prime and $a, m > 1 \in \mathbb{N}$ then

$$\begin{cases} \psi_{(m)} \equiv \lambda - (-1)^\sigma \lambda (mod\ q\ ) \\ \quad if\ \sigma = 1\ and\ a > 1 \in \mathbb{N}\ and\ if\ \sigma = 2\ then\ a\ is\ odd \\ \psi_{(m)} \equiv 2\lambda m^\lambda + \lambda - (-1)^\sigma \lambda (mod\ q\ )\ if\ \sigma = 2\ and\ a\ is\ even \end{cases} \tag{23}$$

Proof. Let be $b = (-1)^\sigma$ From theorem 1 we have

$$\sum_{j=1}^{\lambda-2} \binom{\lambda}{j} ((-1)^\sigma)^{\lambda-j} m^{\lambda-j-1} \equiv \lambda((-1)^\sigma m)^\lambda - \lambda(-m)^\lambda + \lambda - (-1)^\sigma \lambda (\text{mod q}) \tag{24}$$

Let be

$$\psi_{(m)} = \sum_{j=1}^{\lambda-2} \binom{\lambda}{j} ((-1)^\sigma)^{\lambda-\mathrm{j}} m^{\lambda-j-1} \tag{25}$$

From Eq. (24) we get the following

$$\begin{cases} \psi_{(m)} \equiv \lambda - \lambda(-1)^\sigma (mod\ q) \\ if\ \sigma = 1\ and\ a > 1 \in \mathbb{N}\ and\ if\ \sigma = 2\ a\ is\ odd \\ \psi_{(m)} \equiv 2\lambda m^\lambda + \lambda - \lambda(-1)^\sigma (mod\ q) \\ if\ \sigma = 2\ and\ a\ is\ even \end{cases} \tag{26}$$

LEMMA 1. let be $p = 3^m - 2$ and $\mathcal{M} = m3^m - 2m + 1$ where p and $\mathcal{M}$ is a prime number then

$$\sum_{j=1}^{p-2} \pi_j (-2)^{p-j} m^{p-j-1} \equiv \left(2_1^p\right)(-m)^p + 3(mod\ \mathcal{M}) \tag{27}$$

Proof. Let be in theorem 1 $a = 3\ and\ b = -2\ where\ p\ is\ a\ prime$ then we get $\lambda = 3^m - 2\ and\ \mathcal{M} = m3^m - 2m + 1$ and we have

$$\sum_{j=1}^{p-2} \pi_j(-2)^{p-j} m^{p-j-1} \equiv \binom{2^p}{1}(-m)^p + 3(mod\ \mathcal{M}) \tag{28}$$

Then

$$\sum_{j=1}^{M_p-2} \pi_j(-1)^{M_p-j} p^{M_p-j-1} \equiv 2(mod\ \mathcal{M}) \tag{29}$$

LEMMA 2. If F_n fermat number and $p = 2^n F_n + 1$ where p is a prime then

$$\sum_{j=1}^{F_n-2} \pi_j (2^n)^{F_n-j-1} \equiv 2(2^n)^{F_n}(mod\ p) \tag{30}$$

Proof. Let be in theorem 1 $b = 1$ *and* $a = 2$ *and* $m = 2^n$ then we get $\lambda = a^m + b = 2^{2^n} + 1$ and $\mathcal{M} = ma^m + bm + 1 = 2^{2^n+n} + 2^n + 1 = p$ where

$$\sum_{j=1}^{F_n-2} \pi_j (2^n)^{F_n-j-1} \equiv 2(2^n)^{F_n}(mod\ p) \tag{31}$$

REMARK 2: Fermat,s numbers $F_n = 2^{2^n} + 1$ are named after pierre de farmat because he was the first to stud these numbers guess that all fermat numbers are prime

$$3, 5, 17, 57, 65537, \ \dots . \tag{32}$$

But this conjecture was denied by Euler's proved the Fermat number F_5 is not prime

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417 \tag{33}$$

These numbers was named $2^P - 1$ Mersnne numbers, so in Ref. to Marin Meresenne, who began studying them by 2020 he discovered fifty –one prime numbers. There is a program called (the big search for Mersenne prime on the internet). Many prime numbers of Meresnne numbers have been discovered, we know about $M_2, M_3, M_5, M_7, M_{17}, M_{19}, M_{31}, M_{521} \dots, M_{1279}, M_{110305}, M_{132049}, M_{25964951}$ all prime numbers M_{11} is not prime number and they give good results from fermat numbers that only four digits of it have been discovered so far. We know about Fermat numbers, if F_n is not prime, then there is $b = k2^{n+2} + 1$ where F_n/b, and likewise abuot Mersenne numbers, if M_p is not prime, there is $q = 2pr + 1$ where M_p/q and q is prime. From a computational point of view, we find that the results that we have reached are more robust and generalizable those of the results mentioned. Firstly, this is due to the existing ideas and properties is those results. This is represented in highlighting an integral relationship between two prime numbers and more prime numbers. We notice in the LEMMA 1 that the prime numbers and the $p = 3^m - 2$ and the number in form $\mathcal{M} = m3^m - 2m + 1$ numbers in form combine in one result, and also the properties of the Mersnne numbers. Such a correlation does not exist [5, 6] as well as with the ratio of the Fermat numbers also meet with the numbers in LEMMA 2 and this shows relationship between the Fermat numbers and those numbers. In addition to that, the result are expressed a polynomial that highlights the properties of those numbers, and it can also be used as a primitive test to discover those numbers . For a discussion of such issues see [3, 8, 9, 11–14] on there are several numbers studied $A3^n \pm 1, k2^n + 1, 2^n \pm 1$ and close to these formulas.

3. Prime numbers In form $p = am + 1$

In this section we study the prime numbers in form $p = am + 1$ *where* $a, m > 1 \in \mathbb{N}$ which is a special case of the prime numbers form $a^m + bm + 1$, when substituting b a certain value, we study the properties of numbers $p = am + 1, a, m \in \mathbb{N}$ and $q = bp + 1$ *where* $b, p > 1 \in \mathbb{N}$, as well as relationship between polynomial. These polynomial numbers show us special properties of this numbers $am + 1$ as well as the numbers $p = qa + 1$ *where q is a prime number* of the properties, polynomial can be used as a primitive testing algorithm for those numbers. The proof depend mainly on THEOREM 1. In this section, we explain and realize that there is more than one variable in the theorem, for example, $ma^m + bm + 1$ variable $m, a > 1 \in \mathbb{N}$ *and* $b \in \mathbb{Z}, b \neq 0$, because of this, have many distinctive properties. We prove THEOREM 3 is this section and THEOREM 4 by directly changing the value of that variable without any the complexity mentions in particular the basic operations and the binomial theorem are the other extreme in the proofs.

THEOREM 3. *if* $p = qm + 1$ where p, q *is a prime odd* and $a, m > 1 \in \mathbb{N}$ where $C_m(a) = ma^m + 1$ and $\pi_j = \frac{1}{q}\binom{q}{j}$ then

$$\sum_{j=1}^{q-2} \pi_j(-C_m(a))^{q-j-1}(q - a^m) \equiv \chi_{(m,q-a^m)}(mod\ p) \tag{34}$$

Proof. let be in theorem $b = q - a^m$ *where* $q > 2$ *is prime odd* then $\mathcal{M} = ma^m + (q - a^m)m + 1 = qm + 1 = p$ therefore also $\lambda = a^m + b = a^m + q - a^m = q$ so we have that

$$\eta_{(\lambda)}(m, \mathrm{q} - a^m) = \sum_{j=1}^{q-2} \pi_j(q - a^m)^{q-j} m^{q-j-1} \tag{35}$$

And

$$\chi_{(m,q-a^m)} = (mq - ma^m)^{\lambda} - (-m)^{\lambda} - q + a^m + 1 \tag{36}$$

Note that $m(q - a^m) = mq - ma^m = p - ma^m - 1$ *le be* $C_m(a) = ma^m + 1$ then we have

$$\eta_{(q)}(m, q - a^m) = \sum_{j=1}^{q-2} \pi_j(p + (-C_m(a)))^{q-j-1}(q - a^m) \tag{37}$$

Note that from binomial theorem

$$\begin{aligned}&(p+(-C_m(a)))^{q-j-1}\\ &=\sum_{k=0}^{q-j-2}\binom{q-j-1}{k}p^{q-j-1-k}(-C_m(a))^k(q-a^m)\\ &+(-C_m(a))^{q-j-1}(q-a^m)\,\textit{for all}\ 1\le j\le q-1\end{aligned} \tag{38}$$

Let be

$$\psi_m=\sum_{k=1}^{q-j-2}\binom{q-j-1}{k}p^{q-j-1-k}(-C_m(a))^k \tag{39}$$

Then from (37) and (38) and (39) we have

$$\eta_{(q)}(m,q-a^m)=\sum_{j=1}^{q-2}\pi_j\psi_m+\sum_{j=1}^{q-2}\pi_j(-C_m(a))^{q-j-1}(q-a^m) \tag{40}$$

Note that $\psi_m\equiv 0(mod\,p)$ then also

$$\sum_{j=1}^{q-2}\pi_j\psi_m\equiv 0(mod\,p)\ all\ j=1,2,3\dots.q-1 \tag{41}$$

And we know from Eq. (16)

$$\eta_{(q)}(m,q-a^m)\equiv\chi_{(m,q-a^m)}(mod\,p) \tag{42}$$

Now we conclude that from Eqs. (37), (39), and (41) we have

$$\sum_{j=1}^{q-2}\pi_j(-C_m(a))^{q-j-1}(q-a^m)\equiv\chi_{(m,q-a^m)}(mod\,p) \tag{43}$$

From (16) we knew $b=q-a^m$ *then* note that

$$\begin{aligned}\chi_{(m,q-a^m)}&=(mq-ma^m)^q-(-m)^q+1-q+a^m\\ &=(p+(-ma^m-1))^q-(-m)^q-q+a^m+1\\ &=\sum_{j=0}^{q-1}\binom{q}{j}p^{q-j}(-ma^m-1)^j+(-ma^m-1)^q-(-m)^q-q+a^m+1\end{aligned} \tag{44}$$

Note that

$$\sum_{j=0}^{q-1}\binom{q}{j}p^{q-j}(-ma^m-1)^j\equiv 0(mod\,p) \tag{45}$$

If the terms multiplied by variable p are excluded, we get the following

$$\chi_{(m,q-a^m)} = (-ma^m - 1)^q - (-m)^q - q + a^m + 1 \tag{46}$$

Therefore

$$\sum_{j=1}^{q-2} \pi_j(-C_m(a))^{q-j-1}(q-a^m) \equiv \chi_{(m,q-a^m)}(mod\ p) \tag{47}$$

LEMMA 3. *if* $p = 2q + 1$ and q *is a prime odd* then

$$\sum_{j=1}^{q-2} \pi_j\left(-2a^2 - 1\right)^{q-j-1}(q-a^m) \equiv \chi_{(2,q-a^2)}(mod\ p) \tag{48}$$

Proof. Let be in theorem 3 $m = 2$

LEMMA 4. *if* $p = qm + 1$ *and* q *is prime odd and* $m > 1 \in \mathbb{N}$ then

$$\sum_{j=1}^{q-2} \pi_j(-m2^m - 1)^{q-j-1}(q-2^m) \equiv \chi_{(m,q-2^m)}(mod\ p) \tag{49}$$

Proof. Le be in theorem 3 $a = 2$

REMARK 3: if we make a comparison between the results found in [2, 3] about the generalized Cullen numbers and the results that we reached here, in fact, we find that these results are more generalized than those, and also rich in properties than those. The first general and the Cullen numbers in particular, and this is considered one of the properties of the prime numbers of the number in an adjective, as well as this relationship in the form a polynomial that combines the Cullen numbers and the prime number in general $P = qa + 1$ *where* q *is prime odd note* $P \in \mathbb{P} - \{2, 3, 5\}$. Such ideas do not exist in [5, 6, 7, ... .12]. we also note that polynomials can be used as a primitive test to discover prime numbers.

THEOREM 4. *if* $q > 2, m > 1 \in \mathbb{N}$ *and* $p = qm + 1$ and p is prime then

$$\sum_{j=1}^{q-2} \binom{q}{j} (-C_m(a))^{q-j-1}(q-a^m) \equiv \chi_{(q,m,q-a^m)}(mod\ p) \tag{50}$$

Proof. we will prove this theorem with the same ideas as in the proof THEOREM 3 now according THEOREM 1 we have that

$$\eta_{(\lambda)}(b,m) = \sum_{j=1}^{\lambda-2} \binom{\lambda}{j} b^{\lambda-j} m^{\lambda-j-1} \tag{51}$$

And

$$\chi_{(\lambda,b,m)} = \lambda(bm)^{\lambda} - \lambda(-m)^{\lambda} + \lambda - b\lambda \tag{52}$$

Then let be $b = q - a^m$ *and* $m, a, q > 1 \in \mathbb{N}$ where $\lambda = a^m + b = a^m + q - a^m = q$ then we have that

$$\eta_{(q)}(q-a^m,m)=\sum_{j=1}^{q-2}\binom{q}{j}(q-a^m)^{q-j}m^{q-j-1}$$
$$=\sum_{j=1}^{q-2}\binom{q}{j}(p+(-C_m(a)))^{q-j-1}(q-a^m) \tag{53}$$

Then from binomial theorem we conclude that

$$\eta_{(q)}(q-a^m,m)=\sum_{j=1}^{q-2}\binom{q}{j}\sum_{k=0}^{q-j-2}\binom{q-j-1}{j}p^{q-j-1-k}(-C_m(a))^k(q-a^m)$$
$$+\sum_{j=1}^{q-2}\binom{q}{j}(-C_m(a))^{q-j-1}(q-a^m) \tag{54}$$

Note that

$$\sum_{j=1}^{q-2}\binom{q}{j}\sum_{k=0}^{q-j-2}\binom{q-j-1}{j}p^{q-j-1-k}(-C_m(a))^k(q-a^m)\equiv 0(mod\ p) \tag{55}$$

But from theorem 1 we kwon that

$$\eta_{(q)}(q-a^m,m)\equiv\chi_{(\ q,q-a^m,m)}(mod\ p) \tag{56}$$

Then from (54)–(56) we get that

$$\sum_{j=1}^{q-2}\binom{q}{j}(-C_m(a))^{q-j-1}(q-a^m)\equiv\chi_{(\ q,q-a^m,m)}(mod\ p) \tag{57}$$

Note that

$$\chi_{(q,q-a^m,m)}=q(qm-ma^m)^q-q(-m)^q+q-q^2+qa^m \tag{58}$$

Now we have from binomial theorem

$$q(qm-ma^m)^q=q\sum_{j=0}^{q-1}\binom{q}{j}p^{q-j}(-ma^m-1)^j+q(-ma^m-1)^q \tag{59}$$

Note that

$$\sum_{j=0}^{q-1}\binom{q}{j}p^{q-j}(-ma^m-1)^j\equiv 0(mod\ p) \tag{60}$$

Now we are going to eliminate all terms in congruence (60) because it is divisible be p so after that we get the value of $\chi_{(q,q-a^m,m)}$ as follows So we from (56)–(60) we get that

$$\chi_{(q,q-a^m,m)} = q(-ma^m - 1)^q - q(-m)^q + q - q^2 + qa^m \tag{61}$$

Then

$$\sum_{j=1}^{q-2} \binom{q}{j} (-C_m(a))^{q-j-1} (q - a^m) \equiv \chi_{(\ q,q-a^m,m)} (mod\ p) \tag{62}$$

LEMMA 5. *if* $p = 6m + 1$ and $a > 1 \in \mathbb{N}$ then

$$\sum_{j=1}^{4} \binom{6}{j} (-C_m(a))^{5-j} (6 - a^m) \equiv \chi_{(6,m,6-a^m)} (mod\ p\ ) \tag{63}$$

Proof. Let be in theorem 4 $q = 6$

4. Conclusion

We notice theorem 1 that shows us the relationship between the numbers in the form $a^m + b$ and $ma^m + bm + 1$. This is represented by a polynomial that combines these two numbers. One of the benefits of this relationship is that polynomial can be used as a primitive test, as well as clarifying the properties that those numbers have. But from an abstract arithmetic point of view, we find that theorem 3 is in fact more general than the theorem 1, and this is due to theorem 3 combining all the prime numbers. These results are in Cullen numbers and those in [5, 6] we note that these results are more generalized and differ from those in the form of a gem, and this appears and ideas used differ from those in [5, 6 7, ...12,13]. In general, we studied all numbers in from $p = ba + 1$ where $a, b > 1 \in \mathbb{N}$, as well as Mersnne numbers and Cullen numbers, Fermat numbers. We showed about these numbers that have properties and a relationship between them. We proved this relationship in the form of a polynomial that combines two types of prime number or more. We note that only prime numbers in form $p = ba + 1\ where\ a, b > 1 \in \mathbb{N}$ have been studied no more prime numbers in form $p = ba + m\ where\ a, b, m > 1 \in \mathbb{N}$ have not been studied.

Author details

Shazali Abdalla Fadul
Faculty of Mathematics Sciences and Statistics, AL-Neelain University, Khartoum, Sudan

*Address all correspondence to: shazlyabdullah3@gmail.com

References

[1] Rose HS. A Course in Number Theory. 2nd ed. Clarendon Press; 14 Dec 1995. ISBN-10: 0198523769

[2] Grau JM, Oller-Marcén AM. An ~O (log 2(N)) time primality test for generalized Cullen numbers. Mathematics of Computation. 2011;**80** (276):2315-2323. DOI: 10.1090/S0025-5718-2011-02489-0 MR 2813363 6

[3] María GJ, Oller-Marcén Antonio M, Daniel S. A primality test for Kp^n+1 numbers. Mathematics of Computation. 2015;**84**(291):505-512

[4] Bosma W. Cubic Reciprocity and Explicit Primality Tests for $h.3^k \pm 1$ High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie

[5] Pocklington HC. The determination of the prime or composite nature of large numbers by fermat's theorem. Proceedings of the Cambridge Philosophical Society. 1914;**18**:29-30

[6] Williams HC. A note on the primality of $6^{2^n}+1$ and $10^{2^n}+1$. The Fibonacci Quarterly. 1988;**26**(4):296-305 MR 967648

[7] Williams HC, Zarnke CR. Some prime numbers of the forms $2A3^n+1$ and $2A3^n-1$. Mathematics of Computation. 1972;**26**:995-998. MR 314747. DOI: 10.1090/S0025-5718-1972-0314747-X

[8] Berry PBTG, Tena-Ayuso J. A generalization of Proth's theorem. Acta Arithmetica. 2003;**110**(2):107-115. MR 2008078. DOI: 10.4064/aa110-2-1

[9] Berrizbeitia P, Iskra B. Deterministic primality test for numbers of the form $A^2 3^n + 1$ $n > 3$ odd. Proceedings of the American Mathematical Society. 2002; **130**(2):363-365. MR 1862113. DOI: 10.1090/S00029939-01-06100-7

[10] James J. Tattersall Elementary Number Theory in Nine Chapters. Cambridge University Press; 2005. ISBN: 0521850142, 9780521850148

[11] Berrizbeitia P, Berry TG. Generalized strong pseudoprime tests and applications. Journal of Symbolic Computation. 2000;**30**(2):151-160. MR 1777169. DOI: 10.1006/jsco.1999.0343

[12] Berrizbeitia P, Olivieri A. A generalization of Miller's primality theorem. Proceedings of the American Mathematical Society. 2008;**136**(9): 3095-3104. MR 2407072. DOI: 10.1090/S0002-9939-08-09303-9

[13] Crandall R, Pomerance C. Prime Numbers. A Computational Perspective. 2nd ed. New York: Springer; 2005 MR 2156291

[14] Guthmann A. Effective primality tests for integers of the forms $N = k2^n + 1$ and $N = k2^m.3^n + 1$. BIT. 1992;**32**(3): 529-534. MR 1179238. DOI: 10.1007/BF02074886