International Journal of Latest Research in Science and Technology **ISSN (Online):2278-5299**
Volume 3, Issue 5: Page No 26-28. September-October 2014
https://www.mnkpublication.com/journal/ijlrst/index.php

DIVISORS OF NUMBERS OF THE FORM$a^{2^n}+b^{2^n}$

[1]Arto Adili,[2]Lorena Margo
[1]Msc. ArtoAdili, Department of Mathematics, “Fan S. Noli”,University, Korçë,Albania
[2]Msc. Lorena Margo, Department of Mathematics, “Fan S. Noli”, University, Korçë,Albania

***Abstract*- Natural numbers of the form a^2+b^2 have as prime divisors $p=2$ or $p\equiv 1(\mathrm{mod}\,4)$. Basedon this conclusion we can find the general form of all divisors of numbers of the form a^2+b^2. Finding the prime divisors of numbers of the form a^4+b^4, we can find the general form of all divisors of these numbers. Inductively, for any natural number n we can find first the form of all prime divisors of numbers of the form $a^{2^n}+b^{2^n}$ and finally, we can find the general form of all divisors of these numbers.**

***Keywords*–**Divisor, prime number,congruences, Fermat’s Little Theorem

I. INTRODUCTION

Theideafor writingthis article isinspired by particular forms of prime divisors of numbers of the forma^2+b^2, where a and b are positive integers. So, if p is prime number such that $p\,|\,a^2+b^2, a,b\in\mathbb{N}^+$, then $p=2$ or $p\equiv 1(\mathrm{mod}\,4)$.

In this article we will examine the generalised problemwith the divisors of numbers of the form $a^{2^n}+b^{2^n}$, where n is natural number.

We will first find the general form of divisors of numbers of the form a^2+b^2 and a^4+b^4 and finally, the divisors of numbers of the form $a^{2^n}+b^{2^n}$, for any natural number n.

II. DIVISORS OF NUMBERS OF THE FORM a^2+b^2

First, let us consider the following theorem, the proof method of which is obtained by the set of noteson number theory that is written by Naoki Sato for students at the IMO level[1].

We will emphasize particularly that this proof method will be used to find the solution of generalized problems.

Theorem 1. If p is prime number such that $p\,|\,a^2+b^2$, where a and b are positive integers such that $(a,b)=1$, then $p\equiv 1(\mathrm{mod}\,4)$ or $p=2$.

Proof.Since p is a prime number then $p=2$, $p\equiv 1(\mathrm{mod}\,4)$ or $p\equiv 3(\mathrm{mod}\,4)$. To prove the theorem it is sufficient to show that $p\not\equiv 3(\mathrm{mod}\,4)$.

Suppose that $p\equiv 3(\mathrm{mod}\,4)$, namely $p=4k+3$, $k\in\mathbb{N}$. Since $(a,b)=1$and $p\,|\,a^2+b^2$, then $(a,p)=(b,p)=1$. By Fermat’s Little Theorem we have:

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

Since $p\,|\,a^2+b^2$, then $a^2\equiv -b^2(\mathrm{mod}\,p)$ and have

$$a^{p-1}=(a^2)^{2k+1}\equiv(-b^2)^{2k+1}\equiv -b^{p-1}\equiv -1(\mathrm{mod}\,p),$$

which is contradictions. Consequently, $p\not\equiv 3(\mathrm{mod}\,4)$. ■

To find all divisors of numbers of the form a^2+b^2, let us prove now the following theorem:

Theorem 2. If positive integers a and b are both oddnumbers, then $2\,\|\,a^{2^n}+b^{2^n}$ (the number $a^{2^n}+b^{2^n}$ is divisible by 2 but not by 4), for any natural number n.

Proof.We have $a=2a_1+1$, $a_1\in\mathbb{N}$ and

$$a^2=4(a_1^2+a_1)+1\equiv 1(\mathrm{mod}\,4).$$

In the same way $b^2\equiv 1(\mathrm{mod}\,4)$. Since

$$a^{2^n}\equiv a^2\equiv 1(\mathrm{mod}\,4)\text{ and }b^{2^n}\equiv b^2\equiv 1(\mathrm{mod}\,4),$$

it follows that

$$a^{2^n}+b^{2^n}\equiv 2(\mathrm{mod}\,4),$$

namely $2\,\|\,a^{2^n}+b^{2^n}$. ■

If the numbers a and b are both even, then the number a^2+b^2 will be divisible by a power of the number 2, double of the lowest exponent that is present in numbers a and b. This demonstrates that theexponent of number 2 can take as value every even number. Based on this conclusion and Theorem 2 we can say that: if $2^\alpha\,|\,a^2+b^2$, where a and b are positive integers, then α may take as value any natural number.

A prime number$p$, such that $p\equiv 3(\mathrm{mod}\,4)$, will be a divisor of number a^2+b^2, only when the number p divides each of the numbers a and b. This shows that when the prime number $p\equiv 3(\mathrm{mod}\,4)$ is the divisor of the number

Publication History
Manuscript Received : 10 October 2014
Manuscript Accepted : 22 October 2014
Revision Received : 28 October 2014
Manuscript Published : 31 October 2014

a^2+b^2, then its square will be the divisor of number a^2+b^2.
Based on what we stated above it is true the following theorem:

Theorem 3. If M is natural number such that $M \mid a^2+b^2$, where a and b are positive integers, then

$$M = 2^{\alpha}(p_1^{\alpha_1}\dots p_k^{\alpha_k})(q_1^{2\beta_1}\dots q_s^{2\beta_s}),$$

where $p_1, \dots, p_k$ are prime numbers $\equiv 1 (\mathrm{mod}\, 4)$, $q_1, \dots, q_s$ are prime numbers $\equiv 3 (\mathrm{mod}\, 4)$, $k, s \in \mathbb{N}$, $\alpha, \alpha_1, \dots, \alpha_k \in \mathbb{N}$ and $\beta_1, \dots, \beta_s \in \mathbb{N}$. ■

III.DIVISORS OF NUMBER OF THE FORM a^4+b^4

First, let us take the following theorem:

Theorem 4. If p is a prime number such that $p \mid a^4+b^4$, where a and b are positive integers such that $(a, b)=1$, then $p \equiv 1 (\mathrm{mod}\, 8)$ or $p=2$.

Proof. Since p is a prime number then $p \equiv 1, 3, 5, 7 (\mathrm{mod}\, 8)$ or $p=2$. From Theorem 1, we have $p \not\equiv 3, 7 (\mathrm{mod}\, 8)$, so that to prove the theorem it is sufficient to show that $p \not\equiv 5 (\mathrm{mod}\, 8)$.

Suppose that $p \equiv 5 (\mathrm{mod}\, 8)$, namely $p = 8k+5$, $k \in \mathbb{N}$. Since $(a, b)=1$and $p \mid a^4+b^4$, then $(a, p)=(b, p)=1$. By Fermat's Little Theorem we have:

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

Since $p \mid a^4+b^4$, then $a^4 \equiv -b^4 (\mathrm{mod}\, p)$ and have

$$a^{p-1} = (a^4)^{2k+1} \equiv (-b^4)^{2k+1} \equiv -b^{p-1} \equiv -1 (\mathrm{mod}\, p),$$

which is contradictions. Consequently, $p \not\equiv 5 (\mathrm{mod}\, 8)$. ■

If numbers a and b are both even, then the number a^4+b^4 will be divisible by a power of the number 2, four times the lowest exponent that is present in numbers a and b.This demonstrates that the exponent of number 2 can take as value every natural number that is multiple of number 4. Based on this conclusion and Theorem 2 we can say that: if $2^u \mid a^4+b^4$, where a and b are positive integers, then $u = 4\alpha + t$, where $\alpha \in \mathbb{N}$ and $t = 0, 1$.

A prime number p such that $p \equiv 3, 5, 7 (\mathrm{mod}\, 8)$, will be a divisor of number a^4+b^4, only when the number p divide each of the numbers a and b. This show that when the prime number $p \equiv 3, 5, 7 (\mathrm{mod}\, 8)$ is divisor of the number a^4+b^4, then its fourth power will be the divisor of number a^4+b^4.
Based on what we said above it is true the following theorem:

Theorem 5. If M is natural number such that $M \mid a^4+b^4$, where a and b are positive integers, then

$$M = 2^{4\alpha+t}(p_1^{\alpha_1}\dots p_k^{\alpha_k})(q_1^{4\beta_1}\dots q_s^{4\beta_s}),$$

where $p_1, \dots, p_k$ are prime numbers $\equiv 1 (\mathrm{mod}\, 8)$, $q_1, \dots, q_s$ are prime numbers $\equiv 3, 5, 7 (\mathrm{mod}\, 8)$, $t = 0, 1$, $k, s \in \mathbb{N}$, $\alpha, \alpha_1, \dots, \alpha_k \in \mathbb{N}$ and $\beta_1, \dots, \beta_s \in \mathbb{N}$. ■

IV.DIVISORS OF NUMBERS OF THE FORM $a^{2^n}+b^{2^n}$

First, let us take the following theorem:

Theorem 6. If p is a prime number such that $p \mid a^{2^n}+b^{2^n}$, where a, b and n are positive integers such that $(a, b)=1$, then $p \not\equiv 2^n+1 (\mathrm{mod}\, 2^{n+1})$.

Proof. Suppose that $p \equiv 2^n+1 (\mathrm{mod}\, 2^{n+1})$. Then for some $k \in \mathbb{N}$ we have $p = 2^{n+1}k + 2^n + 1$. Since $(a, b)=1$and $p \mid a^{2^n}+b^{2^n}$, then $(a, p)=(b, p)=1$. By Fermat's Little Theorem we have:

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

Since $p \mid a^{2^n}+b^{2^n}$, then $a^{2^n} \equiv -b^{2^n} (\mathrm{mod}\, p)$ and have

$$a^{p-1} = a^{2^{n+1}k+2^n} = a^{2^n(2k+1)} = (a^{2^n})^{2k+1} \equiv (-b^{2^n})^{2k+1} \equiv$$

$$\equiv -(b^{2^n})^{2k+1} \equiv b^{2^{n+1}k+2^n} \equiv -b^{p-1} \equiv -1 (\mathrm{mod}\, p),$$

which is contradictions with $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. Consequently, we have $p \not\equiv 2^n+1 (\mathrm{mod}\, 2^{n+1})$. ■

The following theorem makes it possible to find all prime divisors of number of the form $a^{2^n}+b^{2^n}$.

Theorem 7. If p is a prime number such that $p \mid a^{2^n}+b^{2^n}$, where a and b are positive integers such that $(a, b)=1$, then $p \equiv 1 (\mathrm{mod}\, 2^{n+1})$ or $p=2$.

Proof.We will prove the theorem using the method of complete mathematical inductionby natural number n.

For $n=1$ and $n=2$ the theorem is true based on Theorem 1 and Theorem 4. Assume that the theorem is true for any natural number less than or equal to $n-1$ and let us prove for natural number n.

Since p is prime number then $p=2$ or

$$p \equiv 1, 3, 5, \dots, 2^{n+1}-3, 2^{n+1}-1 (\mathrm{mod}\, 2^{n+1}).$$

Based on the assumption made, will be excluded the values

$$p \equiv 3, 7, \dots, 2^{n+1}-3 (\mathrm{mod}\, 2^{n+1}),$$

because they are of the form $\equiv 3 (\mathrm{mod}\, 4)$, and also excluded the values

$$p \equiv 5, 13, \dots, 2^{n+1}-5 (\mathrm{mod}\, 2^{n+1}),$$

because they are of the form $\equiv 5 (\mathrm{mod}\, 8)$, and so on continue this process until we exclude values

$$p \equiv 2^{n+1}-1, 2^{n+1}-2^n-1 (\mathrm{mod}\, 2^{n+1}),$$

because they are of the form $\equiv 2^n-1 (\mathrm{mod}\, 2^{n+1})$.

The only values that are not excluded are $p \equiv 1(\bmod 2^{n+1})$ and $p \equiv 2^n + 1(\bmod 2^{n+1})$. But, based on the Theorem 6 we have $p \not\equiv 2^n + 1(\bmod 2^{n+1})$, so that finally we have

$$p \equiv 1(\bmod 2^{n+1}) \text{ or } p = 2 . \blacksquare$$

If numbers a and b are both even, then the number $a^{2^n} + b^{2^n}$ will be divisible by a power of the number 2, 2^n-times the lowest exponent that is present in numbers a and b.This demonstrates that the exponent of number 2 can take as value every natural number that is a multiple of the number 2^n. Based on this conclusion and Theorem 2 we can say that: if $2^u \mid a^{2^n} + b^{2^n}$, where a and b are positive integers, then $u = 2^n \alpha + t$, where $\alpha \in □$ and $t = 0 , 1$.

A prime number p, such that

$$p \equiv 3, 5, \dots , 2^{n+1} - 1(\bmod 2^{n+1}) ,$$

will be a divisor of number $a^{2^n} + b^{2^n}$, only when the number p divideseach of the numbers a and b. This shows that when the prime number $p \equiv 3, 5, \dots , 2^{n+1} - 1(\bmod 2^{n+1})$ is a divisor of number $a^{2^n} + b^{2^n}$, then its 2^n-th power will be the divisor of number $a^{2^n} + b^{2^n}$.

Based on whatwe said above it is true the following theorem:

<u>Theorem 8.</u>If M is a natural number such that $M \mid a^{2^n} + b^{2^n}$, where a and b are positive integers, then

$$M = 2^{2^n \alpha + t} (p_1^{\alpha_1} \dots p_k^{\alpha_k})(q_1^{2^n \beta_1} \dots q_s^{2^n \beta_s}) ,$$

where $p_1, \dots , p_k$ are all prime numbers $\equiv 1(\bmod 2^{n+1})$, $q_1, \dots , q_s$ are prime numbers $\equiv 3, 5, \dots , 2^{n+1} - 1(\bmod 2^{n+1})$, $\alpha , \alpha_1, \dots , \alpha_k \in □$, $k , s \in □$, $\beta_1, \dots , \beta_s \in □$ and $t = 0 , 1$. ■

It is obvious that Theorem 3 is a consequence of Theorem 5 and Theorem 5 is a consequence of Theorem 8.

V. CONCLUSIONS

In this paper we found the general form of all divisors of numbers of the form $a^2 + b^2$, where a and b are positive integers, the general form of all divisors of numbers of the form $a^4 + b^4$ and finally the general form of all divisors of numbers of the form $a^{2^n} + b^{2^n}$, for any natural number n.

REFERENCES

[1] Naoki Sato,*Notes on number theory for students at the IMO,* 1995.

[2] A. Adler & J. Coury, *The Theory of Numbers*, Jones and Bartlett.