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

$^1$Arto Adili, $^2$Lorena Margo

$^1$Msc. Arto Adili, 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 $p = 1(mod 4)$. Based on this conclusion we can find the general form of all divisors 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

The idea for writing this article is inspired by particular forms of prime divisors of numbers of the form $a^2 + b^2$, 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 $p = 1(mod 4)$.

In this article we will examine the generalised problem with 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 notes on 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 $p = 1(mod 4)$ or $p = 2$.

**Proof.** Since $p$ is a prime number then $p = 2$, $p = 1(mod 4)$ or $p = 3(mod 4)$. To prove the theorem it is sufficient to show that $p \neq 3(mod 4)$.

Suppose that $p = 3(mod 4)$, 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:

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

Since $p | a^2 + b^2$, then $a^2 = -b^2(mod p)$ and have

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

which is contradictions. Consequently, $p \neq 3(mod 4)$.

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 odd numbers, then $2 || a^2 + b^2$ (the number $a^2 + b^2$ is divisible by 2 but not by 4), for any natural number $n$.

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

$$a^2 = 4(a_i^2 + a_i) + 1 \equiv 1(mod 4).$$

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

$$a^2 = a^2 \equiv 1(mod 4) and b^2 \equiv b^2 \equiv 1(mod 4),$$

it follows that

$$a^2 + b^2 = 2(mod 4),$$

namely $2 || a^2 + b^2$.

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 the exponent of number 2 can take as value every even number. Based on this conclusion and Theorem 2 we can say that: if $2^n | a^2 + b^2$, where $a$ and $b$ are positive integers, then $\alpha$ may take as value any natural number.

A prime number $p$, such that $p = 3(mod 4)$, 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 $p = 3(mod 4)$ is the divisor of the number
Based on what we stated above it is true the following theorem:

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

\[
M = 2^n (p_1^{a_1} \cdots p_k^{a_k}) (q_1^{b_1} \cdots q_l^{b_l})
\]

where \( p_1, \ldots, p_k \) are prime numbers \( \equiv 1 \pmod{4} \), \( q_1, \ldots, q_l \) are prime numbers \( \equiv 3, 7 \pmod{8} \), \( t = 0, 1 \), \( s \in \mathbb{Z} \), \( \alpha, \alpha_1, \ldots, \alpha_k \in \mathbb{Z} \), and \( \beta_1, \ldots, \beta_l \in \mathbb{Z} \).

**IV. DIVISORS OF NUMBERS OF THE FORM \( a^2 + b^5 \)**

First, let us take the following theorem:

**Theorem 6.** If \( p \) is a prime number such that \( p \mid a^2 + b^2 \), where \( a, b \) and \( n \) are positive integers such that \((a, b) = 1\), then \( p \equiv 2^r + 1 \pmod{2^{r+1}} \).

**Proof.** Suppose that \( p = 2^r + 1 \pmod{2^{r+1}} \). Then for some \( k \in \mathbb{Z} \) we have \( p = 2^r k + 2^r + 1 \). Since \((a, b) = 1\) and \( p \mid a^2 + b^2 \), then \((a, p) = (b, p) = 1\). By Fermat’s Little Theorem we have:

\[
a^{p-1} = b^{p-1} = 1 \pmod{p}.
\]

Since \( a \mid a^2 + b^2 \), then \( a = 2^b \pmod{p} \) and have

\[
a^{p-1} = (a^2)^{2k-1} = (-b^2)^{2k-1} = -b^{p-1} = -1 \pmod{p},
\]

which is contradictions. Consequently, \( p \not\equiv 2^r + 1 \pmod{2^{r+1}} \).

If numbers \( a \) and \( b \) are both even, then the number \( a^2 + b^2 \) 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 \( 2^n \mid a^2 + b^2 \), where \( a \) and \( b \) are positive integers, then \( u = 4a + t \), where \( u \in \mathbb{Z} \) and \( t = 0, 1 \).

A prime number \( p \) such that \( p = 3, 5, 7 \pmod{8} \), will be a divisor of number \( a^2 + b^2 \), only when the number \( p \) divide each of the numbers \( a \) and \( b \). This show that when the prime number \( p = 3, 5, 7 \pmod{8} \) is divisor of the number \( a^2 + b^2 \), then its fourth power will be the divisor of number \( a^2 + b^2 \).

Based on what we said above it is true the following theorem:

**Theorem 5.** If \( M \) is a natural number such that \( M \mid a^2 + b^2 \), where \( a \) and \( b \) are positive integers, then

\[
M = 2^{4u} (p_1^{a_1} \cdots p_k^{a_k}) (q_1^{b_1} \cdots q_l^{b_l}),
\]

where \( p_1, \ldots, p_k \) are prime numbers \( \equiv 1 \pmod{4} \), \( q_1, \ldots, q_l \) are prime numbers \( \equiv 3, 7 \pmod{8} \), \( t = 0, 1 \), \( s \in \mathbb{Z} \), \( \alpha, \alpha_1, \ldots, \alpha_k \in \mathbb{Z} \), and \( \beta_1, \ldots, \beta_l \in \mathbb{Z} \).
The only values that are not excluded are \( p \equiv 1(\text{mod} \ 2^{n+1}) \) and 
\( p = 2^n + 1(\text{mod} \ 2^{n+1}) \). But, based on the Theorem 6 we have 
\( p \not\equiv 2^n + 1(\text{mod} \ 2^{n+1}) \), so that finally we have 
\[ p \equiv 1(\text{mod} \ 2^{n+1}) \text{ or } p = 2. \]

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 \( 2^n | a^{2^n} + b^{2^n} \), where \( a \) and \( b \) are positive integers, then \( u = 2^n \alpha + t \), where \( \alpha \in \mathbb{Z} \) and \( t = 0,1 \).

A prime number \( p \), such that 
\[ p = 3,5,\ldots,2^n+1-l(\text{mod} \ 2^{n+1}) \],
will be a divisor of number \( a^{2^n} + b^{2^n} \), only when the number \( p \) divides each of the numbers \( a \) and \( b \). This shows that when the prime number \( p = 3,5,\ldots,2^n+1-l(\text{mod} \ 2^{n+1}) \) 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 what we said above it is true the following theorem:

**Theorem 8.** If \( M \) is a natural number such that \( M | a^{2^n} + b^{2^n} \), where \( a \) and \( b \) are positive integers, then
\[ M = 2^{n+1} (p_1^{\alpha_1} \ldots p_k^{\alpha_k})(q_1^{2^{2\alpha_1}} \ldots q_s^{2^{2\alpha_s}}), \]
where \( p_1,\ldots,p_k \) are all prime numbers \( \equiv 1(\text{mod} \ 2^{n+1}) \),
\( q_1,\ldots,q_s \) are prime numbers \( \equiv 3,5,\ldots,2^n+1-l(\text{mod} \ 2^{n+1}) \),
\( \alpha,\alpha_1,\ldots,\alpha_k \in \mathbb{Z}, k,s \in \mathbb{Z}, \beta_1,\ldots,\beta_s \in \mathbb{Z} \) 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**
