

ON PRIME NUMBERS OF THE FORM $a^2 + ab + b^2$, WHERE $a \in \mathbb{N}^+, b \in \mathbb{N}^+$

Arno Mikaelyan, Nairi Sedrakyan, Hayk Sedrakyan

Abstract

Let $\mathbb{N}^+$ stand for the set of all natural numbers and 0. In this paper we investigate prime numbers of the form $a^2 + ab + b^2$, where $a \in \mathbb{N}^+, b \in \mathbb{N}^+$, and some novel properties related to them. We prove that any number of the form $c^2 + 3d^2$, where $c \in \mathbb{N}^+, d \in \mathbb{N}^+$ can be represented in the form $a^2 + ab + b^2$, where $a \in \mathbb{N}^+, b \in \mathbb{N}^+$. We prove that any prime number p of the form $p = 6n + 1$, where $n \in \mathbb{N}$ can be represented in the form $c^2 + 3d^2$, where $c \in \mathbb{Z}, d \in \mathbb{Z}$. We also prove that any prime number p of the form $p = 6n + 5$, where $n \in \mathbb{N}$ cannot be represented in the form $a^2 + ab + b^2$ where $a \in \mathbb{Z}, b \in \mathbb{Z}$.

Main results and proofs

Problem 1. Prove that

$$\{a^2 + 3b^2 | a \geq 0, b \geq 0, a \in \mathbb{Z}, b \in \mathbb{Z}\} = \{a^2 + ab + b^2 | a \geq 0, b \geq 0, a \in \mathbb{Z}, b \in \mathbb{Z}\}.$$

Proof. From equation $a^2 + 3b^2 = |a|^2 + 3|b|^2$ follows that

$$\{a^2 + 3b^2 | a \geq 0, b \geq 0, a \in \mathbb{Z}, b \in \mathbb{Z}\} = \{a^2 + 3b^2 | a \in \mathbb{Z}, b \in \mathbb{Z}\}.$$

And $|a| \cdot |b| = ab$ or $|a| \cdot |b| = -ab$. Let us use the following identity

$$|a|^2 - |a| \cdot |b| + |b|^2 = (|a| - |b|)^2 + |b|(|a| - |b|) + |b|^2.$$

From this equation we get

$$\{a^2 + ab + b^2 | a \geq 0, b \geq 0, a \in \mathbb{Z}, b \in \mathbb{Z}\} = \{a^2 + ab + b^2 | a \in \mathbb{Z}, b \in \mathbb{Z}\}.$$

$$M = \{a^2 + 3b^2 | a \in \mathbb{Z}, b \in \mathbb{Z}\}.$$

$$K = \{a^2 + ab + b^2 | a \in \mathbb{Z}, b \in \mathbb{Z}\}.$$

We need to prove that $M = K$. Let $x \in M$, then $x = a^2 + 3b^2$, where $a, b \in \mathbb{Z}$.

According to $a^2 + 3b^2 = (a + b)^2 + (a + b)(-2b) + (-2b)^2$ identity, $x \in K$. Then $x = a^2 + ab + b^2$, where $a, b \in \mathbb{Z}$.

Let us consider a case where a or b is an even number. If b is an even number then

$$x = a^2 + ab + b^2 = \left(a + \frac{b}{2}\right)^2 + 3\left(\frac{b}{2}\right)^2$$

therefore $x \in M$. Let us consider a case where a and b are odd numbers. According to the following identity

$$a^2 + ab + b^2 = \left(\frac{a-b}{2}\right)^2 + 3\left(\frac{a+b}{2}\right)^2,$$

we have $x \in M$. Thus, if $x \in K$, then $x \in M$. This ends the proof.

Problem 2. Prove that if $x \in M$ and $y \in M$, then $xy \in M$.

Proof. We have $x = a^2 + 3b^2$, $y = c^2 + 3d^2$ where $a, b, c, d \in \mathbb{Z}$

According to the following identity

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2,$$

we get that $xy \in M$. This ends the proof.

Problem 3. Prove that if x is even and $x \in M$, then $4|x$ and $\frac{x}{4} \in M$.

Proof. We have $x = a^2 + 3b^2$ and a and b integer numbers have the same parity according to the following identity

$$\frac{a^2 + 3b^2}{4} = \left(\frac{a - 3b}{2}\right)^2 + 3\left(\frac{a + b}{2}\right)^2,$$

we get that $4|x$ and $x \in M$. This ends the proof.

Problem 4. Prove that if $x \in M$, $p \in M$ (p is prime) and $p|x$, then $\frac{x}{p} \in M$.

Proof. We have $x = a^2 + 3b^2$, $p = c^2 + 3d^2$, where a, b, c, d are integers.

$$xp = (a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2 = (ac + 3bd)^2 + 3(ad - bc)^2. (1)$$

Also

$$(ad + bc)(ac + 3bd) = cd(a^2 + 3b^2) + ab(c^2 + 3d^2) = cd \cdot x + ab \cdot p$$

is divisible by p . Therefore, either $p|ad + bc$ or $p|ac + 3bd$. When $p|ad + bc$, we get (1) that $p|ac - 3bd$ and

$$\frac{x}{p} = \left(\frac{ac - 3bd}{p}\right)^2 + 3\left(\frac{ad + bc}{p}\right)^2 \in M.$$

When $p|ac + 3bd$ and $p \neq 3$ we again get (1) that $p|ad - bc$ and

$$\frac{x}{p} = \left(\frac{ac + 3bd}{p}\right)^2 + 3\left(\frac{ad - bc}{p}\right)^2 \in M.$$

When $p = 3$, from equation $x = a^2 + 3b^2$ and $3|x$ condition, we get $3|a$.

Let $a = 3a_1$, where a_1 is an integer number. Therefore $\frac{x}{3} = 3a_1^2 + b^2 \in M$. This ends the proof.

Problem 5. Prove that if $x \in M$, y is an odd natural number $y \notin M$ and $y|x$, then $\frac{x}{y}$ has at least one odd positive divisor that does not belong to M .

Proof. Let $\frac{x}{y} = 2^m \cdot p_1 \cdot \dots \cdot p_k$ are odd prime numbers.

We proceed the proof by contradiction argument. Assume that **all** odd positive divisors of $\frac{x}{y}$ belong to M .

Therefore $p_1, \dots, p_k \in M$, according to problem 4 we have

$$\frac{x}{p_1}, \frac{x}{p_1 p_2}, \dots, \frac{x}{p_1 \dots p_k} \in M.$$

Since $\frac{x}{p_1} \in M$ and p_2 is a divisor of $\frac{x}{p_1}$ therefore according to problem 4 we have

$$\frac{\frac{x}{p_1}}{p_2} \in M.$$

We get

$$\frac{\frac{x}{p_1}}{p_2} = \frac{x}{p_1 p_2} \in M.$$

In a similar way, we get that

$$\frac{x}{p_1 p_2 p_3}, \dots, \frac{x}{p_1 \dots p_k} \in M.$$

According to problem 3, if $x \in M$ and $x = 2^m \cdot Z$, where Z is an odd number, then $\frac{x}{2^m} \in M$, therefore we get that $y = \frac{x}{p_1 \dots p_k} \div 2^m \in M$. This leads to a contradiction, as given that $y \notin M$. This ends the proof.

Problem 6. Prove that if a and b natural numbers are relatively prime, then every odd divisor of $a^2 + 3b^2$ belongs to M .

Proof. Let $a^2 + 3b^2$ have an odd divisor, which does **not** belong to M . Consider

$$M_1 = \{c^2 + 3d^2 | c, d \in \mathbb{N}, \text{ GCD}(c, d) = 1\}.$$

Note that $a^2 + 3b^2 \in M_1$. Let m be the smallest positive odd number that is a divisor of some element of the set M_1 and $m \notin M$.

Let $m|u^2 + 3v^2$ (1), where $u > 0, v > 0$ and $GCD(u, v) = 1$. Perform division with remainder $u = mq_1 + r_1, v = mq_2 + r_2$, where $|r_1| < \frac{m}{2}$ and $|r_2| < \frac{m}{2}$.

Now, let us prove that $m|r_1^2 + 3r_2^2$. From condition (1) we have $m|u^2 + 3v^2$. Given that $u = mq_1 + r_1, v = mq_2 + r_2$. Thus, we get

$$\begin{aligned} u^2 + 3v^2 &= (mq_1 + r_1)^2 + 3(mq_2 + r_2)^2 = m^2q_1^2 + 2mq_1r_1 + r_1^2 + 3(m^2q_2^2 + 2mq_2r_2 + r_2^2) = \\ &= m^2q_1^2 + 2mq_1r_1 + 3m^2q_2^2 + 6mq_2r_2 + r_1^2 + 3r_2^2. \end{aligned}$$

We get that

$$m|m(mq_1^2 + 2q_1r_1 + 3mq_2^2 + 6q_2r_2) + (r_1^2 + 3r_2^2).$$

Hence $m|(r_1^2 + 3r_2^2)$. So, $r_1^2 + 3r_2^2 = m \cdot n$. We have $|r_1| < \frac{m}{2}$ and $|r_2| < \frac{m}{2}$, thus

$$mn < \frac{m^2}{4} + \frac{3m^2}{4} = m^2.$$

Thus, $n < m$. If p is such prime that $p|r_1$ and $p|r_2$, then from $p|m$ we get $p|u$ and $p|v$. This leads to a contradiction, as we have $GCD(u, v) = 1$. So, m is not divisible by p . Then, $p|n$. We have $r_1^2 + 3r_2^2 = m \cdot n$, dividing both sides by p^2 , we get

$$\left(\frac{r_1}{p}\right)^2 + 3\left(\frac{r_2}{p}\right)^2 = m \cdot \frac{n}{p^2}.$$

Let us use problem 5, where we take $x = (\frac{r_1}{p})^2 + 3(\frac{r_2}{p})^2$ and $y = m$, then we get

$$\frac{x}{y} = \frac{(\frac{r_1}{p})^2 + 3(\frac{r_2}{p})^2}{m}$$

So according to problem 5 we have $\frac{x}{y}$ has an odd divisor that does not belong to M . On the other hand, we have

$$\frac{x}{y} = \frac{n}{p^2}.$$

Thus, $\frac{n}{p^2}$ has an odd divisor that does not belong to M . So, n has an odd divisor that does not belong to M . This leads to a contradiction, as that odd divisor of n is smaller than m (but m is the smallest such number). This ends the proof.

Problem 7. Let $p = 6n + 1$, where $n \in \mathbb{N}$ and p is prime. Prove that $p \in M$.

Proof. We proceed the proof by contradiction argument. Assume that $p \notin M$.

Let us consider the numbers $1^{6n}, 2^{6n}, \dots, (6n)^{6n}$, note that

$$(i+1)^{6n} - i^{6n} = (i+1)^{6n} - 1 - (i^{6n} - 1)$$

is divisible by p , where $i \in \{1, 2, \dots, 6n-1\}$. On the other hand, we have

$$(i+1)^{6n} - i^{6n} = ((i+1)^{2n} - i^{2n})((i+1)^{4n} + (i+1)^{2n} \cdot i^{2n} + i^{4n}),$$

and $(i+1)^{4n} + (i+1)^{2n} \cdot i^{2n} + i^{4n} \in M$. If

$$p|(i+1)^{4n} + (i+1)^{2n} \cdot i^{2n} + i^{4n},$$

then according to problem 6 we get that $p \in M$. Because from numbers $(i+1)^{2n}$ and i^{2n} only one is even and $A^2 + 2AB + 4B^2 = (A+B)^2 + 3B^2$, where $GCD(A, B) = 1$. Thus, it follows that $GCD(A+B, B) = 1$.

It remains to prove the claim when $p|(i+1)^{2n} - i^{2n}$ where $i = 1, 2, \dots, 6n$. It is known that $(x-1)^{2n} \cdot k^{2n} = (2n)!$, therefore from these two facts we get $p|(2n)!$, which is impossible. This ends the proof.

From problems 1 and 7 we get that there exist positive integers a and b so that $a^2 + ab + b^2 = p$, where p is any prime number of the form $6n + 1$, $n \in \mathbb{N}$.

Problem 8. Prove that a prime number of the form $6n + 5$, for $n \in \{0, 1, 2, \dots\}$, cannot be represented in the form $a^2 + ab + b^2$, where $a \in \mathbb{Z}$, $b \in \mathbb{Z}$.

Proof. Let us proceed with the proof by contradiction argument. Assume that $p = 6n + 5$ ($n \in \mathbb{Z}$) be a prime number and $p = a^2 + ab + b^2$, where $a, b \in \mathbb{Z}$. Note that a and b cannot be simultaneously divisible by p because $p = (pa_1)^2 + pa_1 \cdot pb_1 + (pb_1)^2 = p^2(a_1^2 + a_1b_1 + b_1^2)$ is impossible. Moreover, none of the numbers a and b is divisible by p because if we assume that only a is divisible by p we will get that b is also divisible by p , as $p = (pa_1)^2 + pa_1b + b^2$. Hence, we get that $p(1 - (pa_1^2 + a_1b)) = b^2$.

According to Fermat's little theorem, we have $p|(a^{p+1} - a^2)$ and $p|(b^{p+1} - b^2)$. Subtracting the last expression from the first expression, we get

$$p|((a^{p+1} - b^{p+1}) - (a^2 - b^2)) \quad (1)$$

On the other hand $a^{p+1} - b^{p+1} = a^{6n+6} - b^{6n+6}$, therefore $(a^3 - b^3)|a^{p+1} - b^{p+1}$, moreover $(a^2 + ab + b^2)|(a^3 - b^3)$. Thus $p|(a^{p+1} - b^{p+1})$, therefore from (1) we get that $p|(a^2 - b^2)$. (2)

From (2) we get that $p|(a - b)(a + b)$. Let us assume that both $(a - b)$ and $(a + b)$ are simultaneously divisible by p . If we add them we will get that $p|2a$ which is possible only if $p = 2$ but since $p = 6n + 5$ it is impossible.

We have $p = (a - b)^2 + 3ab = (a + b)^2 - ab$ and from the last equation and from (2) we obtain $p|(ab)$, which is impossible. Thus $p \notin K$. This ends the proof.

Note that prime number p belongs to K if $p = 3$ or p leaves a remainder of 1 when divided by 6.