Accepted Manuscript

Prime numbers p with expression $p = a^2 \pm ab \pm b^2$

Kamal Bahmanpour

PII: S0022-314X(16)30031-2
DOI: http://dx.doi.org/10.1016/j.jnt.2016.02.024
Reference: YJNTH 5411

To appear in: *Journal of Number Theory*

Received date: 18 November 2015
Revised date: 10 February 2016
Accepted date: 11 February 2016

Please cite this article in press as: K. Bahmanpour, Prime numbers p with expression $p = a^2 \pm ab \pm b^2$, *J. Number Theory* (2016), http://dx.doi.org/10.1016/j.jnt.2016.02.024

Highlights

- For any pair of integers m and n, define $K_{m,n} := \{a^2 + mab + nb^2 \mid m, n \in \mathrm{Z}\}$.
- $K_{m,n}$ is a semi-group, for any pair of integers m and n.
- A prime number p can be expressed as $p = a^2 \pm ab - b^2$ with integers a and b, if and only if, p is congruent to 0, 1 and -1 modulo 5.
- A prime number p can be expressed as $p = a^2 \pm ab + b^2$ with integers a and b, if and only if, p is congruent to 0 and 1 modulo 3.

Prime numbers p with expression $p = a^2 \pm ab \pm b^2$[☆]

Kamal Bahmanpour

Faculty of Mathematical Sciences, Department of Mathematics, University of Mohaghegh Ardabili, 56199-11367, Ardabil, Iran; and School of Mathematics, Institute for Research in Fundamental Sciences (IPM), P.O. Box. 19395-5746, Tehran, Iran.

Abstract

Let p be a prime number. In this paper we show that p can be expressed as $p = a^2 \pm ab - b^2$ with integers a and b if and only if p is congruent to 0, 1 or -1 (mod 5) and p can be expressed as $p = a^2 \pm ab + b^2$ with integers a and b if and only if p is congruent to 0, 1 (mod 3).

Keywords: binary quadratic form, finite group, Law of Quadratic Reciprocity, prime number, semi-group.
2010 MSC: 11D41, 11D72.

1. Introduction

Fermat stated in 1640 that an odd prime p can represented by the binary quadratic form $a^2 + b^2$ with integers a and b if and only if p is congruent to 1 (mod 4). This was first proved by Euler in two papers published in 1753 and 1755, (see [2] and [3]). But the standard simpler proof one can find in most introductory books in number theory is essentially due to Lagrange, and is partly similar to his proof of the four squares theorem, (see [1]). Since then, many different proofs have been found. Among them, the Zagier's short proof based on involutions (see [7]), have appeared.

Binary quadratic forms and their prime representations have been studied by several authors. Lagrange was the first to give a complete treatment of the topic, and various mathematicians, including Legendre, Euler and Gauss, contributed to the theory. In this paper we study the binary quadratic forms $a^2 \pm ab \pm b^2$. More precisely, we show that a prime number p can be expressed as $p = a^2 \pm ab - b^2$ with integers a and b if and only if p is congruent to 0, 1 or -1 (mod 5) and p can be expressed as $p = a^2 \pm ab + b^2$ with integers a and b if and only if p is congruent to 0, 1 (mod 3). Our methods of proof in some parts of it is based on adaptation of Lagrange's technique for the two and four

[☆]This research of the author was supported by a grant from IPM (No. 94130022).
Email address: bahmanpour.k@gmail.com (Kamal Bahmanpour)

squares theorems.

For any unexplained notation and terminology, we refer to [1] and [4].

2. Preliminaries

The following results will be useful in the proof of Lemmata 3.1 and 3.6.

Lemma 2.1. *Let m and n be two integers. Let ξ_1, ξ_2 be the roots of the equation $x^2 + mx + n = 0$. Then for each pair of integers a and b we have*

$$a^2 + mab + nb^2 = (a - b\xi_1)(a - b\xi_2).$$

Proof. Put $x = \frac{a}{b}$ in the relation $x^2 + mx + n = (x - \xi_1)(x - \xi_2)$. □

In the following result, we shall show that the set of all integers in Lagrange's quadratic form $a^2+mab+nb^2$, $a, b \in \mathbb{Z}$, composes a semi-group with usual product of integers.

Theorem 2.2. *Let m and n be two integers and let $\mathfrak{K}_{m,n} := \{a^2 + mab + nb^2 : a, b \in \mathbb{Z}\}$. Then $(\mathfrak{K}_{m,n}, \times)$ is a semi-group.*

Proof. Let α and β be elements of $\mathfrak{K}_{m,n}$. Then there are integers a, b, c, d such that $\alpha = a^2 + mab + nb^2$ and $\beta = c^2 + mcd + nd^2$. Let ξ_1 and ξ_2 be the roots of the equation $x^2 + mx + n = 0$. Then we have $\xi_i^2 = -m\xi_i - n$, for $i = 1, 2$. Now, using Lemma 2.1 we have

$$\begin{aligned}
\alpha\beta &= (a^2 + mab + nb^2)(c^2 + mcd + nd^2) \\
&= (a - b\xi_1)(c - d\xi_1)(a - b\xi_2)(c - d\xi_2) \\
&= [(ac) - (bc + ad)\xi_1 + bd\xi_1^2][(ac) - (bc + ad)\xi_2 + bd\xi_2^2] \\
&= [(ac) - (bc + ad)\xi_1 + bd(-m\xi_1 - n)] \\
&\quad \times[(ac) - (bc + ad)\xi_2 + bd(-m\xi_2 - n)] \\
&= [(ac - nbd) - (bc + ad + mbd)\xi_1][(ac - nbd) - (bc + ad + mbd)\xi_2] \\
&= (ac - nbd)^2 + m(ac - nbd)(bc + ad + mbd) + n(bc + ad + mbd)^2,
\end{aligned}$$

which implies that $\alpha\beta \in \mathfrak{K}_{m,n}$. □

Lemma 2.3. *Let p be a prime number such that $p \equiv \pm 1 \pmod 5$. Then there exists an integer $a \in \{1, 2, ..., \frac{p-1}{2}\}$, such that $a^2 - a - 1 = tp$, for some positive integer $1 \leq t < p$.*

Proof. Since by hypothesis we have $p \equiv \pm 1 \pmod 5$ and each of the integers 1 and -1 are quadratic residue modulo 5, it follows from the Law of Quadratic Reciprocity that there is an integer b such that $b^2 \equiv 5 \pmod p$. On the other

hand there is an element $c \in \{0, 1, 2, ..., p-1\}$ such that $c \equiv b \pmod{p}$. So, we have $c^2 \equiv 5 \pmod{p}$ and $(p-c)^2 \equiv 5 \pmod{p}$. Since p is an odd number it follows that one of the integers c or $p-c$ is an odd number. So, there is a positive integer a such that $2a-1 \in \{0, 1, 2, ..., (p-1)\}$ and $(2a-1)^2 \equiv 5 \pmod{p}$. Therefore, $4a^2 - 4a - 4 \equiv 0 \pmod{p}$. Since $(4, p) = 1$ it follows that $a^2 - a - 1 \equiv 0 \pmod{p}$. So, there is an integer t such that $a^2 - a - 1 = tp$. Since a is an integer it follows that $t \neq 0$. Moreover, since $p \geq 11$, it follows that $a \geq 4$ and hence we have

$$a^2 - a - 1 = (a - \frac{1}{2})^2 - \frac{5}{4} > 3^2 - 2 = 7 > 0.$$

Therefore, we have $t \geq 1$. Moreover, since $1 \leq 2a - 1 \leq p - 2$ then we have $1 \leq a \leq \frac{p-1}{2}$. Now, we have

$$t = \frac{a^2 - a - 1}{p} < \frac{(\frac{p}{2})^2 + (\frac{p}{2}) + 1}{p} = \frac{p}{4} + \frac{1}{2} + \frac{1}{p} < \frac{p}{4} + 1 < p.$$

Therefore, we have $1 \leq t < p$. □

Lemma 2.4. *Let p be a prime number such that $p \equiv 1 \pmod{3}$. Then there exists an integer $a \in \{0, \pm 1, \pm 2, ..., \pm(\frac{p-1}{2})\}$ such that $a^3 \equiv 1 \pmod{p}$, but $a \not\equiv 1 \pmod{p}$. In particular, there is a positive integer $1 \leq t < p$ such that $a^2 + a + 1 = tp$.*

Proof. The group $(\mathbb{Z}_p^{\times}, \odot)$ is of finite order $\varphi(p) = p - 1$, where φ is the Euler's function. Moreover, by hypothesis we have $3|(p-1)$. Therefore, in view of Cauchy's theorem, (see [5]), the group $\mathbb{Z}_p^{\times}$ contains an element $\overline{c}$ of order 3. Now, there exists an integer $a \in \{0, \pm 1, \pm 2, ..., \pm(\frac{p-1}{2})\}$ such that $c \equiv a \pmod{p}$. Now, it is clear that $a^3 \equiv 1 \pmod{p}$, but $a \not\equiv 1 \pmod{p}$. Thus, using the factorization $a^3 - 1 = (a-1)(a^2 + a + 1)$ and the fact that $p \not| (a-1)$, it follows that there is an integer t such that $a^2 + a + 1 = tp$. But we have $a^2 + a + 1 = (a + \frac{1}{2})^2 + \frac{3}{4} > 0$, which implies that $t > 0$ and hence $t \geq 1$. Moreover, since by hypothesis we have $|a| \leq \frac{p-1}{2}$, it follows that

$$t = \frac{a^2 + a + 1}{p} \leq \frac{(\frac{p}{2})^2 + (\frac{p}{2}) + 1}{p} = \frac{p}{4} + \frac{1}{2} + \frac{1}{p} < \frac{p}{4} + 1 < p.$$

Therefore, we have $1 \leq t < p$. □

Remark 2.5. *According to the referee's suggestion, using the proof of Lemma 2.3, one can find an easy alternative proof for the Lemma 2.4, based on the Law of Quadratic Reciprocity, instead of using Cauchy's theorem. In fact, we need just the following argument. If $p \equiv 1 \pmod{3}$, then -3 is a quadratic residue modulo p, and thus there is an integer $a \in \{0, \pm 1, \pm 2, ..., \pm(p-1)/2\}$ such that $(2a+1)^2 \equiv -3 \pmod{p}$.* □

3. Main results

In this section we will prove our main results, Theorems 3.4 and 3.9. But, first we need the following lemma.

Lemma 3.1. *Let p be a prime number such that $p \equiv \pm 1 \pmod 5$. Then there are integers a, b such that $p = a^2 - ab - b^2$.*

Proof. Let $\mathfrak{K}_{-1,-1}$ be as in Theorem 2.2. By Lemma 2.3, there are integers $1 \leq t < p$ and $1 \leq d \leq \frac{p-1}{2}$ such that

$$tp = d^2 - d - 1 = d^2 - d(1) - (1)^2 \in \mathfrak{K}_{-1,-1}.$$

Let

$$\mathfrak{B} := \{k \in \mathbb{N} \ : \ 1 \leq k < p \text{ and } kp \in \mathfrak{K}_{-1,-1}\}.$$

Then as $t \in \mathfrak{B}$, it follows that $\mathfrak{B} \neq \emptyset$. It is enough to prove $1 \in \mathfrak{B}$. Assume the opposite and let ℓ be the smallest element of $\mathfrak{B}$. Then we have $1 < \ell < p$ and there are integers e and f such that $\ell p = e^2 - ef - f^2$. Now, we can find integers e_0 and f_0 such that

$$e_0 \equiv e \,(\mathrm{mod}\, \ell) \quad \text{and} \quad f_0 \equiv f \,(\mathrm{mod}\, \ell)$$

and

$$|e_0| \leq \frac{\ell}{2} \quad \text{and} \quad |f_0| \leq \frac{\ell}{2}.$$

In this situation we claim that it is impossible that we have $e_0 = f_0 = 0$. Because, if we have this relation, then we have $e \equiv f \equiv 0 \pmod \ell$ and so $e^2 \equiv ef \equiv f^2 \equiv 0 \pmod{\ell^2}$. Thus, we must have $\ell p = e^2 - ef - f^2 \equiv 0 \pmod{\ell^2}$, which implies that $\ell | p$ and this is a contradiction. Because, we have $1 < \ell < p$. So, we have $e_0 \neq 0$ or $f_0 \neq 0$. Now, we claim that it is impossible that we have $e_0^2 - e_0 f_0 - f_0^2 = 0$. Assume the opposite and let $s = (e_0, f_0)$. Then there are integers e_1 and f_1 such that $e_0 = se_1$, $f_0 = sf_1$ and $(e_1, f_1) = 1$. Then from the relation $e_0^2 - e_0 f_0 - f_0^2 = 0$ we conclude the relation $e_1^2 - e_1 f_1 - f_1^2 = 0$. Now we consider the following two cases. In the first case, we may assume $e_0 \neq 0$. Then we have $e_1 \neq 0$ and $e_1 | f_1^2$. So, we must have $e_1 = \pm 1$. Then we have $1 \pm f_1 - f_1^2 = 0$ which is impossible. In second case we may assume $f_0 \neq 0$. Then we have $f_1 \neq 0$ and $f_1 | e_1^2$. So, we must have $f_1 = \pm 1$. Then we have $e_1^2 \pm e_1 - 1 = 0$ which is impossible. So, we have $e_0^2 - e_0 f_0 - f_0^2 \neq 0$. Now, we consider the following two cases.

Case 1. Assume that $e_0^2 - e_0 f_0 - f_0^2 > 0$. Then we have $e_0^2 - e_0 f_0 - f_0^2 \geq 1$. On the other hand, we have

$$e_0^2 - e_0 f_0 - f_0^2 \equiv e^2 - ef - f^2 \equiv 0 \,(\mathrm{mod}\, \ell).$$

Therefore, there exists a positive integer m such that

$$e_0^2 - e_0 f_0 - f_0^2 = \ell m.$$

Moreover, we have

$$\begin{aligned} m &= \frac{e_0^2 - e_0 f_0 - f_0^2}{\ell} \\ &\leq \frac{e_0^2 + |e_0||f_0| + f_0^2}{\ell} \\ &\leq \frac{(\frac{\ell}{2})^2 + (\frac{\ell}{2})^2 + (\frac{\ell}{2})^2}{\ell} \\ &= \frac{3}{4}\ell < \ell. \end{aligned}$$

So, we have $1 \leq m < \ell$.
Next, by using the proof of Theorem 2.2, we have

$$\begin{aligned} \ell^2 mp &= (\ell m)(\ell p) = -(e_0^2 - e_0 f_0 - f_0^2)(f^2 + fe - e^2) \\ &= -(e_0^2 - e_0 f_0 - f_0^2)(f^2 - f(-e) - (-e)^2) \\ &= -[(e_0 f - e f_0)^2 - (f_0 f - e_0 e + f_0 e)(e_0 f - e f_0) \\ &\quad -(f_0 f - e_0 e + f_0 e)^2]. \end{aligned}$$

Now, we have

$$e_0 f - e f_0 \equiv ef - ef \equiv 0 \,(\mathrm{mod}\, \ell)$$

and

$$f_0 f - e_0 e + f_0 e \equiv f^2 - e^2 + ef = -(e^2 - ef - f^2) \equiv 0 \,(\mathrm{mod}\, \ell).$$

Therefore,

$$\alpha = \frac{e_0 f - e f_0}{\ell} \quad \text{and} \quad \beta = \frac{f_0 f - e_0 e + f_0 e}{\ell},$$

are integers such that

$$mp = -[\alpha^2 - \alpha\beta - \beta^2] = \beta^2 - (-\alpha)(\beta) - (-\alpha)^2 \in \mathfrak{K}_{-1,-1}$$

and $1 \leq m < \ell$, which means $m \in \mathfrak{B}$ and m is smaller than the smallest element of $\mathfrak{B}$, which is a contradiction.

Case 2. Assume that $e_0^2 - e_0 f_0 - f_0^2 < 0$. Then we have

$$-(e_0^2 - e_0 f_0 - f_0^2) = f_0^2 - (-e_0) f_0 - (-e_0)^2 \geq 1.$$

On the other hand, we have

$$f_0^2 - (-e_0) f_0 - (-e_0)^2 = -(e_0^2 - e_0 f_0 - f_0^2) \equiv -(e^2 - ef - f^2) \equiv 0 \,(\mathrm{mod}\, \ell).$$

Therefore, there exists a positive integer m such that

$$f_0^2 - (-e_0) f_0 - (-e_0)^2 = \ell m.$$

Moreover, we have

$$\begin{aligned} m &= \frac{f_0^2 - (-e_0)f_0 - (-e_0)^2}{\ell} \\ &\leq \frac{e_0^2 + |e_0||f_0| + f_0^2}{\ell} \\ &\leq \frac{(\frac{\ell}{2})^2 + (\frac{\ell}{2})^2 + (\frac{\ell}{2})^2}{\ell} \\ &= \frac{3}{4}\ell < \ell. \end{aligned}$$

So, we have $1 \leq m < \ell$.
Next, by using the proof of Theorem 2.2, we have

$$\begin{aligned} \ell^2 mp &= (\ell m)(\ell p) = -(e_0^2 - e_0 f_0 - f_0^2)(e^2 - ef - f^2) \\ &= (f_0^2 - (-e_0)f_0 - (-e_0)^2)(e^2 - ef - f^2) \\ &= [(f_0 e - e_0 f)^2 - (-e_0 e + f_0 f + e_0 f)(f_0 e - e_0 f) \\ &\quad -(-e_0 e + f_0 f + e_0 f)^2]. \end{aligned}$$

Now, we have

$$f_0 e - e_0 f \equiv fe - ef \equiv 0 \,(\mathrm{mod}\, \ell)$$

and

$$-e_0 e + f_0 f + e_0 f \equiv -e^2 + f^2 + ef = -(e^2 - ef - f^2) \equiv 0 \,(\mathrm{mod}\, \ell).$$

Therefore,

$$\alpha = \frac{f_0 e - e_0 f}{\ell} \quad \text{and} \quad \beta = \frac{-e_0 e + f_0 f + e_0 f}{\ell},$$

are integers such that

$$mp = \alpha^2 - \alpha\beta - \beta^2 \in \mathfrak{K}_{-1,-1}$$

and $1 \leq m < \ell$, which means $m \in \mathfrak{B}$ and m is smaller than the smallest element of $\mathfrak{B}$, which is a contradiction. □

The following consequence of Lemma 3.1 is needed in the proof of Theorem 3.4.

Corollary 3.2. *A prime number p can be expressed as $p = a^2 - ab - b^2$ with integers a and b, whenever p is congruent to 0, -1 or 1 (mod 5).*

Proof. If $p \equiv 0 \,(\mathrm{mod}\, 5)$, then $p = 5$ and we can find integers $a = 3$ and $b = 1$ with the desired property. Also, if we have $p \equiv 1$ or $-1 \,(\mathrm{mod}\, 5)$, then the assertion holds by Lemma 3.1. □

The next result is needed in the proof of our first main result.

Lemma 3.3. *Let p be a prime number and $\mathfrak{K}_{-1,-1}$ be as in Theorem 2.2. If $p \in \mathfrak{K}_{-1,-1}$, then $p \equiv 1$, -1 or $0 \pmod 5$.*

Proof. By hypothesis there are integers a, b such that $p = a^2 - ab - b^2$. In this situation we claim that it is impossible that we have $a \equiv b \pmod p$. Assume the opposite. Then we have $a \equiv b \pmod p$. Therefore, we have $-a^2 \equiv -b^2 \equiv a^2 - ab - b^2 = p \equiv 0 \pmod p$. So, we have $p|a$ and $p|b$. Hence, we have

$$p^2|(a^2 - ab - b^2) = p,$$

which is a contradiction. So, we have $a \not\equiv b \pmod p$. Also, it is easy to see that $(a, p) = 1 = (b, p)$. Thus in the field $(\mathbb{Z}_p, \oplus, \odot)$, we have $(\overline{c})^2 - \overline{c} - \overline{1} = \overline{0}$, where $\overline{c} = \overline{a}(\overline{b})^{-1}$ and so $(2c - 1)^2 \equiv 5 \pmod p$. Now, it follows from the Law of Quadratic Reciprocity that $p \equiv 1$, -1 or $0 \pmod 5$. □

Now we are ready to state and prove our first main result in this paper.

Theorem 3.4. *A prime number p can be expressed as $p = a^2 - ab - b^2$ with integers a and b, if and only if p is congruent to 0, 1 or $-1 \pmod 5$.*

Proof. The assertion follows from Corollary 3.2 and Lemma 3.3. □

Remark 3.5. *It is clear that a prime number p can be expressed as $p = a^2 - ab - b^2$ with integers a and b, if and only if, p can be expressed as $p = c^2 + cd - d^2$ with integers c and d. So, it follows from the Theorem 3.4 that, a prime number p can be expressed as $p = a^2 + ab - b^2$ with integer a and b, if and only if p is congruent to 0, 1 or $-1 \pmod 5$.*

According to the referee suggestion, the method used in the proof of Theorem 3.4 also can be applied for the prime numbers with representation by the binary quadratic form $a^2 \pm ab + b^2$. This binary quadratic form for fist time has been verified by *U. P. Nair*, (see [6]). In fact our proof for the Theorem 3.9 is an alternative proof for his result.

Lemma 3.6. *Let p be a prime number such that $p \equiv 1 \pmod 3$. Then there are integers a, b such that $p = a^2 + ab + b^2$.*

Proof. Let $\mathfrak{K}_{1,1}$ be as in Theorem 2.2. By Lemma 2.4 there are integers $1 \leq t < p$ and $-(\frac{p-1}{2}) \leq d \leq \frac{p-1}{2}$ such that

$$tp = d^2 + d + 1 = d^2 + d(1) + (1)^2 \in \mathfrak{K}_{1,1}.$$

Let

$$\mathfrak{B} := \{k \in \mathbb{N} \ : \ 1 \leq k < p \text{ and } kp \in \mathfrak{K}_{1,1}\}.$$

Then as $t \in \mathfrak{B}$, it follows that $\mathfrak{B} \neq \emptyset$. It is enough to prove $1 \in \mathfrak{B}$. Assume the opposite and let ℓ be the smallest element of $\mathfrak{B}$. Then we have $1 < \ell < p$

and there are integers e and f such that $\ell p = e^2 + ef + f^2$. Now, we can find integers e_0 and f_0 such that

$$e_0 \equiv e \,(\mathrm{mod}\, \ell) \quad \text{and} \quad f_0 \equiv f \,(\mathrm{mod}\, \ell)$$

and

$$|e_0| \leq \frac{\ell}{2} \quad \text{and} \quad |f_0| \leq \frac{\ell}{2}.$$

In this situation we claim that it is impossible that we have $e_0 = f_0 = 0$. Because, if we have this relation, then we have $e \equiv f \equiv 0 \pmod{\ell}$ and so $e^2 \equiv ef \equiv f^2 \equiv 0 \pmod{\ell^2}$. Thus, we must have $\ell p = e^2 + ef + f^2 \equiv 0 \pmod{\ell^2}$, which implies that $\ell | p$ and this is a contradiction. Because, we have $1 < \ell < p$. So, without loss of generality we may assume that $f_0 \neq 0$. Then, since

$$e_0^2 + e_0 f_0 + f_0^2 = (e_0 + \frac{f_0}{2})^2 + \frac{3}{4} f_0^2 > 0,$$

it follows that $e_0^2 + e_0 f_0 + f_0^2 \geq 1$. On the other hand, we have

$$e_0^2 + e_0 f_0 + f_0^2 \equiv e^2 + ef + f^2 \equiv 0 \,(\mathrm{mod}\, \ell).$$

Therefore, there exists a positive integer m such that

$$e_0^2 + e_0 f_0 + f_0^2 = \ell m.$$

Moreover, we have

$$\begin{aligned} m &= \frac{e_0^2 + e_0 f_0 + f_0^2}{\ell} \\ &\leq \frac{e_0^2 + |e_0||f_0| + f_0^2}{\ell} \\ &\leq \frac{(\frac{\ell}{2})^2 + (\frac{\ell}{2})^2 + (\frac{\ell}{2})^2}{\ell} \\ &= \frac{3}{4}\ell < \ell. \end{aligned}$$

So, we have $1 \leq m < \ell$.
Next, by using the proof of Theorem 2.2, we have

$$\begin{aligned} \ell^2 mp &= (\ell m)(\ell p) = (e_0^2 + e_0 f_0 + f_0^2)(f^2 + fe + e^2) \\ &= [(e_0 f - e f_0)^2 + (f_0 f + e_0 e + f_0 e)(e_0 f - e f_0) \\ &\quad + (f_0 f + e_0 e + f_0 e)^2]. \end{aligned}$$

Now, we have

$$e_0 f - e f_0 \equiv ef - ef \equiv 0 \,(\mathrm{mod}\, \ell)$$

and

$$f_0 f + e_0 e + f_0 e \equiv f^2 + e^2 + ef \equiv 0 \,(\mathrm{mod}\, \ell).$$

Therefore,

$$\alpha = \frac{e_0 f - e f_0}{\ell} \quad \text{and} \quad \beta = \frac{f_0 f + e_0 e + f_0 e}{\ell},$$

are integers such that

$$mp = \alpha^2 + \alpha\beta + \beta^2 \in \mathfrak{K}_{1,1}$$

and $1 \leq m < \ell$, which means $m \in \mathfrak{B}$ and m is smaller than the smallest element of $\mathfrak{B}$, which is a contradiction. □

The following consequence of Lemma 3.6 is needed in the proof of Theorem 3.9.

Corollary 3.7. *A prime number p can be expressed as $p = a^2 + ab + b^2$ with integers a and b, whenever p is congruent to* 0 *or* 1 (mod 3).

Proof. If $p \equiv 0 \pmod 3$, then $p = 3$ and we can find $a = b = 1$ with the desired property. Also, if we have $p \equiv 1 \pmod 3$, then the assertion holds by Lemma 3.6. □

The next result is needed in the proof of our second main result.

Lemma 3.8. *Let $p \neq 3$ be a prime number and $\mathfrak{K}_{1,1}$ be as in Theorem 2.2. If $p \in \mathfrak{K}_{1,1}$, then $p \equiv 1 \pmod 3$.*

Proof. By hypothesis there are integers a, b such that $p = a^2 + ab + b^2$. In this situation we claim that it is impossible that we have $a \equiv b \pmod p$. Assume the opposite. Then we have $a \equiv b \pmod p$. Therefore, we have $3a^2 \equiv 3b^2 \equiv a^2 + ab + b^2 = p \equiv 0 \pmod p$. So, as by hypothesis we have $p \neq 3$, it follows that $p|a$ and $p|b$. Hence, we have

$$p^2 | (a^2 + ab + b^2) = p,$$

which is a contradiction. So, we have $a \not\equiv b \pmod p$. Also, it is easy to see that $(a, p) = 1 = (b, p)$. Thus in finite group $(\mathbb{Z}_p^\times, \odot)$, we have $\overline{a}(\overline{b})^{-1} \neq \overline{1}$ and $(\overline{a}(\overline{b})^{-1})^3 = \overline{1}$. So, the finite group $\mathbb{Z}_p^\times$ has an element $\overline{c} = \overline{a}(\overline{b})^{-1}$ of order 3. So, it follows from the Lagrange's theorem that $3|\varphi(p) = p - 1$, where φ is the Euler's function. Hence, we have $p \equiv 1 \pmod 3$. □

Now we are ready to state and prove the second main result of this paper.

Theorem 3.9. *A prime number p can be expressed as $p = a^2 + ab + b^2$ with integers a and b, if and only if p is congruent to* 0 *or* 1 (mod 3).

Proof. The assertion follows from Corollary 3.7 and Lemma 3.8. □

Remark 3.10. *It is clear that a prime number p can be expressed as $p = a^2 + ab + b^2$ with integers a and b, if and only if, p can be expressed as $p = c^2 - cd + d^2$ with integers c and d. So, it follows from the Theorem 3.9 that, a prime number p can be expressed as $p = a^2 - ab + b^2$ with integer a and b, if and only if p is congruent to* 0, 1 (mod 3).

Acknowledgments

The author is deeply grateful to the referee for a very careful reading of the manuscript and many valuable suggestions and for drawing the author's attention to Lemma 2.4, Lemma 3.6 and Theorem 3.9. He also, would like to acknowledge his deep gratitude from Professor Amirgholi Soleimani for his encouragement during writing this paper. Finally, the author would like to thank from School of Mathematics, Institute for Research in Fundamental Sciences (IPM) for its financial support, (grant No. 94130022).

References

[1] W. W. Adams and L. J. Goldstein, *Introduction to Number Theory*, Prentice - Hall, Inc, (1976).

[2] *De numerus qui sunt aggregata quorum quadratorum.* Novi commentarii academiae scientiarum Petropolitanae, **4**, (1752/3, published 1758), 3–40.

[3] *Demonstratio theorematis FERMATIANI omnem numerum primum formae* $4n + 1$ *esse summam duorum quadratorum.* Novi commentarii academiae scientiarum Petropolitanae, **5**, (1754/5, published 1760), 3–13.

[4] M. Hall, *The Theory of Groups*, New York: The Macmillan Company, (1959).

[5] J. McKay, *Another proof of Cauchy's group theorem*, Amer. Math. Monthly., **66**, (1959), 119.

[6] U. P. Nair, *Elementary results on the binary quartratic form* $a^2 + ab + b^2$, (2004), arXiv:math/0408107 [math.NT].

[7] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \ mod \ 4$ *is a sum of two squares*, Amer. Math. Monthly., **97** (1990), 144.