Journal of Number Theory 166 (2016) 208–218

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

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

Kamal Bahmanpour [a,b]

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

ARTICLE INFO

Article history:
Received 18 November 2015
Received in revised form 10 February 2016
Accepted 11 February 2016
Available online 1 April 2016
Communicated by David Goss

MSC:
11D41
11D72

Keywords:
Binary quadratic form
Finite group
Law of quadratic reciprocity
Prime number
Semi-group

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 $-1 \pmod 5$ 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, $1 \pmod 3$.

☆ This research of the author was supported by a grant from IPM (No. 94130022).
E-mail address: bahmanpour.k@gmail.com.

http://dx.doi.org/10.1016/j.jnt.2016.02.024
0022-314X/

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 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