Stud. Univ. Babeş-Bolyai Math. 58(2013), No. 4, 421–430

Primes of the form $\pm a^2 \pm qb^2$

Eugen J. Ionascu and Jeff Patterson

To the memory of Professor Mircea-Eugen Craioveanu (1942-2012)

Abstract. Representations of primes by simple quadratic forms, such as $\pm a^2 \pm qb^2$, is a subject that goes back to Fermat, Lagrange, Legendre, Euler, Gauss and many others. We are interested in a comprehensive list of such results, for $q \leq 20$. Some of the results can be established with elementary methods and we exemplify that in some instances. We are introducing new relationships between various representations.

Mathematics Subject Classification (2010): 11E25, 11A41, 11A67.

Keywords: Quadratic reciprocity, Pigeonhole principle.

1. Introduction

Let us consider the following three types of representations for a natural number:

$$\mathcal{E}(q) := \{n \in \mathbb{N} | n = a^2 + qb^2, \text{ with } a, b \in \mathbb{Z}\}, \tag{1.1}$$

$$\mathcal{H}_1(q) := \{n \in \mathbb{N} | n = qb^2 - a^2, \text{ with } a, b \in \mathbb{Z}\}, \text{ and} \tag{1.2}$$

$$\mathcal{H}_2(q) := \{n \in \mathbb{N} | n = a^2 - qb^2, \text{ with } a, b \in \mathbb{Z}\}. \tag{1.3}$$

We are going to denote by $\mathcal{P}$ the set of prime numbers. In this paper we want to exemplify how standard elementary methods can be used to obtain the representations stated in the next three theorems:

Theorem 1.1. *For a prime p we have $p \in \mathcal{E}(q)$ if and only if*

(I) *(Fermat) ($q = 1$) $p = 2$ or $p \equiv 1$ (mod 4)*
(II) *(Fermat) ($q = 2$) $p = 2$ or $p \equiv 1$ or 3 (mod 8)*
(III) *(Fermat-Euler) ($q = 3$) $p = 3$ or $p \equiv 1$ (mod 6)*
(IV) *($q = 4$) $p \equiv 1$ (mod 4)*
(V) *(Lagrange) ($q = 5$) $p = 5$ or $p \equiv j^2$ (mod 20) for some $j \in \{1, 3\}$*
(VI) *($q = 6$) $p \equiv 1$ or 7 (mod 24)*
(VII) *($q = 7$) $p = 7$ or $p \equiv j^2$ (mod 14) for some $j \in \{1, 3, 5\}$*
(VIII) *($q = 8$) $p \equiv 1$ (mod 8)*
(IX) *($q = 9$) $p \equiv j^2$ (mod 36) for some $j \in \{1, 5, 7\}$*

(x) $(q = 10)$ $p \equiv j \pmod{40}$ for some $j \in \{1, 9, 11, 19\}$
(xi) $(q = 12)$ $p \equiv j \pmod{48}$ for some $j \in \{1, 13, 25, 37\}$
(xii) $(q = 13)$ $p \equiv j^2 \pmod{52}$ for some $j \in \{1, 3, 5, 7, 9, 11\}$
(xiii) $(q = 15)$ $p \equiv j \pmod{60}$ for some $j \in \{1, 19, 31, 49\}$
(xiv) $(q = 16)$ $p \equiv 1 \pmod 8$

We are going to prove (VII), in order introduce the method that will be employed several times. One may wonder what is the corresponding characterization for $q = 11$ or $q = 14$. It turns out that an answer cannot be formulated only in terms of residue classes as shown in ([19]). We give in Theorem 1.4 possible characterizations whose proofs are based on non-elementary techniques which are described in [6].

Theorem 1.2. *For a prime p we have $p \in \mathcal{H}_1(q)$ if and only if*
(i) $(q = 1)$ $p \neq 2$
(ii) $(q = 2)$ $p = 2$ or $p \equiv \pm 1 \pmod 8$ (i.e. $p \equiv 1$ or $p \equiv 1 \pmod 8$)
(iii) $(q = 3)$ $p \in \{2, 3\}$ or $p \equiv 11 \pmod{12}$
(iv) $(q = 4)$ $p \equiv 3 \pmod 4$
(v) $(q = 5)$ $p = 5$ or $p \equiv \pm j^2 \pmod{20}$ for some $j \in \{1, 3\}$
(vi) $(q = 6)$ $p = 2$ or $p \equiv j \pmod{24}$ for some $j \in \{5, 23\}$
(vii) $(q = 7)$ $p = 7$ or $p \equiv j \pmod{14}$ for some $j \in \{3, 5, 13\}$
(viii) $(q = 8)$ $p = 7$ or $p \equiv -j^2 \pmod{32}$ for some $j \in \{1, 3, 5, 7\}$
(ix) $(q = 9)$ $p \equiv -1 \pmod 6$
(x) $(q = 10)$ $p \equiv j \pmod{40}$ for some $j \in \{1, 9, 31, 39\}$
(xi) $(q = 11)$ $p \in \{2, 11\}$ or $p \equiv -j^2 \pmod{44}$ for some $j \in \{1, 3, 5, 7, 9\}$

In this case, for exemplification, we show (V).

Theorem 1.3. *For a prime p we have $p \in \mathcal{H}_2(q)$ if and only if*
(i) $(q = 1)$ $p \neq 2$
(ii) $(q = 2)$ $p = 2$ or $p \equiv \pm 1 \pmod 8$
(iii) $(q = 3)$ $p \equiv 1 \pmod{12}$
(iv) $(q = 4)$ $p \equiv 1 \pmod 4$
(v) $(q = 5)$ $p = 5$ or $p \equiv \pm j^2 \pmod{20}$ for some $j \in \{1, 3\}$
(vi) $(q = 6)$ $p = 3$ or $p \equiv j \pmod{24}$ for some $j \in \{1, 19\}$
(vii) $(q = 7)$ $p = 2$ or $p \equiv j \pmod{14}$ for some $j \in \{1, 9, 11\}$
(viii) $(q = 8)$ $p = 7$ or $p \equiv j^2 \pmod{32}$ for some $j \in \{1, 3, 5, 7\}$
(ix) $(q = 9)$ $p \equiv 1 \pmod 6$
(x) $(q = 10)$ $p \equiv j \pmod{40}$ for some $j \in \{1, 9, 31, 39\}$
(xi) $(q = 11)$ $p \equiv j^2 \pmod{44}$ for some $j \in \{1, 3, 5, 7, 9\}$

We observe that for $q = 2$, $q = 5$, $q = 10$ the same primes appear for both characterizations in Theorem 1.2 and Theorem 1.3. There are several questions that can be raised in relation to this observation:
Problem 1. Determine all values of q, for which we have

$$\mathcal{H}_1(q) \cap \mathcal{P} = \mathcal{H}_2(q) \cap \mathcal{P}. \tag{1.4}$$

Problem 2. If the equality (1.4) holds true for relatively prime numbers q_1 and q_2, does is it hold true for $q_1 q_2$?

In [6], David Cox begins his classical book on the study of (1.1), with a detailed and well documented historical introduction of the main ideas used and the difficulties encountered in the search of new representations along time. The following abstract characterization in [6] brings more light into this subject:

(Theorem 12.23 in [6]**)** *Given a positive integer q, there exists an irreducible polynomial with integer coefficients f_q of degree $h(-4q)$, such that for every odd prime p not dividing q,*

$$p = a^2 + qb^2 \Leftrightarrow \text{the equations} \begin{cases} x^2 \equiv -q \ (mod\ p) \\ \\ f_q(x) \equiv 0 \ (mod\ p) \end{cases}$$

have integer solutions. An algorithm for computing f_q exists. ($h(D)$ is the number of classes of primitive positive definite quadratic forms of discriminant D).

While some of the representations included here are classical, others may be more or less known. We found some of the polynomials included here by computational experimentations. For more details in this direction see [1], [2], [5], [6], [7], [15] and [19].

Theorem 1.4. *For an odd prime p we have $p = a^2 + qb^2$ for some integers a, b if and only if*

(I) *($q = 11$) $p > 2$ and the equation*

$$(X^3 + 2X)^2 + 44 \equiv 0 \ (mod\ p) \quad \text{has a solution,}$$

(II) *(Euler's conjecture) ($q = 14$) the equations*

$$X^2 + 14 \equiv 0 \text{ and } (X^2 + 1)^2 - 8 \equiv 0 \ (mod\ p) \text{ have solutions}$$

(III) *($q = 17$) the equations $X^2 + 17 \equiv 0$ and $(X^2 - 1)^2 + 16 \equiv 0$ (mod p) have solutions*

(IV) *($q = 18$) the equation $(X^2 - 3)^2 + 18(2^2) \equiv 0$ (mod p) has a solution*

(V) *($q = 19$) the equation $(X^3 - 4x)^2 + 19(4^2) \equiv 0$ (mod p) has a solution*

(VI) *($q = 20$) the equation $(X^4 - 4)^2 + 20X^4 \equiv 0$ (mod p) has a solution*

(XXI) *($q = 21$) the equation $(X^4 + 4)^2 + 84X^4 \equiv 0$ (mod p) has a solution*

(XXII) *($q = 22$) $p > 22$ and the equation $(x^2 + 3)^2 + 22(4^2) \equiv 0$ (mod p) has a solution*

(XXIII) *($q = 23$) the equation $(X^3 + 15X)^2 + 23(19^2) \equiv 0$ (mod p) has a solution*

(XXIV) *($q = 24$) the equation $(X^4 + 4)^2 + 24(2X)^4 \equiv 0$ (mod p) has a solution*

(XXV) *($q = 25$) $p > 25$ the equation $X^4 + 100 \equiv 0$ (mod p) has a solution*

(XXVI) *($q = 26$)*

(XXVII) *(Gauss) ($q = 27$) $p \equiv 1$ (mod 3) and the equation $X^3 \equiv 2$ (mod p) has a solution*

(XXVIII) *($q = 28$)*

(XXVIV) *($q = 29$) $p \equiv 1$ (mod 4) and the equation $(X^3 - X)^2 + 116 = 0$ (mod p)*

has a solution

(xxx) *($q = 30$)*

(xxxi) *($q = 31$) (L. Kronecker, pp. 88 [6]) the equation*

$$(X^3 - 10X)^2 + 31(X^2 - 1)^2 \equiv 0 \ (mod\ p) \ \text{ has a solution}$$

(xxxii) *($q = 32$) $p \equiv 1$ (mod 8) and the equation*

$$(X^2 - 1)^2 \equiv -1 \ (mod\ p) \ \text{has a solution.}$$

(xxxvii) *($q = 37$) the equation $X^4 + 31X^2 + 9 = 0$ (mod p) has a solution*

(lxiv) *(Euler's conjecture) ($q = 64$) $p \equiv 1$ (mod 4) and the equation $X^4 \equiv 2$ (mod p) has a solution.*

Our interest in this subject came from studding the problem of finding all equilateral triangles, in the three dimensional space, having integer coordinates for their vertices (see [3], [8], [9], and [12]). It turns out that such equilateral triangles exist only in planes $\mathcal{P}_{a,b,c,f} := \{(x, y, z) \in \mathbb{R}^3 : ax + by + cz = f, f \in \mathbb{Z}\}$ where a, b, and c are in such way

$$a^2 + b^2 + c^2 = 3d^2 \tag{1.5}$$

for some integer d and side-lengths of the triangles are of the form

$$\ell = d\sqrt{2(m^2 - mn + n^2)}$$

for some integers m and n. Let us include here a curious fact that we ran into at that time.

Proposition 1.5. [8] *An integer t which can be written as $t = 3x^2 - y^2$ with $x, y \in \mathbb{Z}$ is the sum of two squares if and only if t is of the form $t = 2(m^2 - mn + n^2)$ for some integers m and n.*

If we introduce the sets

$$A := \{t \in \mathbb{Z} | t = 3x^2 - y^2, x, y \in \mathbb{Z}\},$$

$$B := \{t \in \mathbb{Z} | t = x^2 + y^2, x, y \in \mathbb{Z}\}$$

and

$$C := \{t \in \mathbb{Z} | t = 2(x^2 - xy + y^2), x, y \in \mathbb{Z}\}$$

then we actually have an interesting relationship between these sets.

Theorem 1.6. *For the sets defined above, one has the inclusions*

$$A \cap B \subsetneqq C, \quad B \cap C \subsetneqq A, \quad \text{and} \quad C \cap A \subsetneqq B. \tag{1.6}$$

We include a proof of this theorem in the Section 4. The inclusions in (1.6) are strict as one can see from Figure 1.

Let us observe that there are primes p with the property that $2p$ is in all three sets A, B and C. We will show that these primes are the primes of the form $12k + 1$

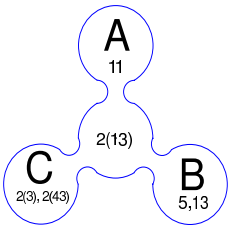

FIGURE 1. *"God created the integers, all else is the work of man." Leopold Kronecker*

for some integer k. Some representations for such primes are included next:

$$13 = (1^2 + 5^2)/2 = 3^2 - 3(4) + 4^2 = [3(3^2) - 1]/2$$

$$37 = (5^2 + 7^2)/2 = 3^2 - 3(7) + 7^2 = [3(5)^2 - 1]/2 \tag{1.7}$$

$$61 = (1^2 + 11^2)/2 = 4^2 - 4(9) + 9^2 = [3(9^2) - 11^2]/2.$$

It is natural to ask whether or not the next forms in the Theorem 1.1 aren't related to similar parameterizations for regular or semi-regular simplices in $\mathbb{Z}^n$ for bigger values of n. In [20], Isaac Schoenberg gives a characterization of those n's for which a regular simplex exists in $\mathbb{Z}^n$. Let us give the restatement of Schoenberg's result which appeared in [16]: *all n such that $n+1$ is a sum of 1, 2, 4 or 8 odd squares.*

As interesting corollaries of these statements we see that if one prime p has some representation it must have some other type of representation(s). Let us introduce a notation for these classes of primes:

$$\mathcal{P}_q := \{p \text{ odd prime} | p = a^2 + qb^2 \text{ for some } a, b \in \mathbb{N}\}.$$

So we have $\mathcal{P}_1 = \mathcal{P}_4$, $\mathcal{P}_8 = \mathcal{P}_{16}$ (Gauss, see [21]), $\mathcal{P}_5 \subset \mathcal{P}_1$, $\mathcal{P}_{10} \subset \mathcal{P}_2$, ... In the same spirit, we must bring to reader's attention, that in the case $q = 32$ there exists a characterization due to Barrucand and Cohn [1], which can be written with our notation as

$$\mathcal{P}_{32} = \{p \mid p \equiv 1 \ (mod\ 8), \text{there exists } x \text{ such that } x^8 \equiv -4 \ (mod\ p)\}.$$

We observe that (**xxxii**) in Theorem 1.4 implies this characterization because $x^8 + 4 = (x^4 - 2x^2 + 2)(x^4 + 2x^2 + 2)$ and clearly $(x^2 - 1)^2 + 1 = x^4 - 2x^2 + 2$. In fact, the two statements are equivalent. Indeed, if a is a solution of $x^8 + 4 \equiv 0$ (mod p) then we either have $x^4 - 2x^2 + 2 \equiv 0$ (mod p) or $x^4 + 2x^2 + 2 \equiv 0$ (mod p). We know that there exists a solution b of $x^2 + 1 \equiv 0$ (mod p). Hence if $a^4 + 2a^2 + 2 \equiv 0$ (mod p) then $(ab)^4 - 2(ab)^2 + 2 \equiv 0$ (mod p) which shows that the equation $x^4 - 2x^2 + 2 \equiv 0$ (mod p) always has a solution.

Also, another classical result along these lines is Kaplansky's Theorem ([14]):

Theorem 1.7. *A prime of the form $16n+9$ is in $\mathcal{P}_{32} \setminus \mathcal{P}_{64}$ or in $\mathcal{P}_{64} \setminus \mathcal{P}_{32}$. For a prime p of the form $16n+1$ we have $p \in \mathcal{P}_{32} \cap \mathcal{P}_{64}$ or $p \notin \mathcal{P}_{64} \cup \mathcal{P}_{32}$.*

For further developments similar to Kaplansky's result we refer to [2]. One can show that the representations in Theorem 1.1 are unique (see Problem 3.23 in [6]).

2. Case (vii)

We are going to use elementary methods in the next three sections and the well known Law of Reciprocity.

Theorem 2.1. **[Gauss]** *For every p and q odd prime numbers we have*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{2.1}$$

with notation $\left(\frac{\cdot}{p}\right)$, defined for every odd prime p and every a coprime with p known as the Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if the equation } x^2 \equiv a \pmod p \text{ has a solution,} \\ \\ -1 \text{ if the equation } x^2 \equiv a \pmod p \text{ has no solution} \end{cases} \tag{2.2}$$

We think that this method can be used to prove all the statements in Theorem 1.1, Theorem 1.3 and Theorem 1.2. We learned about this next technique from [17] and [18].

Necessity. If $p = x^2 + 7y^2$ then $p \equiv x^2 \pmod 7$. Clearly we may assume $p > 7$. Therefore, x may be assumed to be different of zero. Then the residues of $p \pmod 7$ are 1, 2, or 4. Let us suppose that $p \equiv r \pmod{14}$ with $r \in \{0, 1, 2, ..., 13\}$. Because p is prime, r must be an odd number, not a multiple of 7 and which equals 1, 2 or 4 (mod 7). This leads to only three such residues, i.e. $r \in \{1, 9, 11\}$, which are covered by the odd squares j^2, $j \in \{1, 3, 5\}$.

Sufficiency. We may assume that $p > 2$. Let us use the hypothesis to show that the equation $x^2 = -7$ has a solution. Let p be a prime of the form $14k + r$, $r \in \{1, 9, 11\}$, $k \in \mathbb{N} \cup \{0\}$. By the Quadratic Reciprocity, we have $\left(\frac{7}{p}\right)\left(\frac{p}{7}\right) = (-1)^{\frac{3(p-1)}{2}}$. Since $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, then

$$\left(\frac{-7}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}+\frac{3(p-1)}{2}}\left(\frac{p}{7}\right) = \left(\frac{r'}{7}\right),$$

where $p = 7(2k') + r', r' \in \{0, 1, .., 6\}$. This shows that if $r' \in \{1, 2, 4\}$ we have a solution x_0 for the equation $x^2 \equiv -7 \pmod p$.

Let us now apply the Pigeonhole Principle: we let $m \in \mathbb{N}$ be in such a way that $m^2 < p < (m+1)^2$. We consider the function $g : \{0, 1, 2, ..., m\} \times \{0, 1, 2, ..., m\} \to \{0, 1, 2, ..., p-1\}$ defined by $g(u, v) \equiv u + vx_0 \pmod p$. Since $(m+1)^2 > p$, we must have two distinct pairs (a'', b'') and (a', b') such that $g(a'', b'') = g(a', b')$. Then $a'' - a' \equiv (b' - b'')x_0 \pmod p$. Then, if we let $a = a'' - a'$, and $b = b' - b''$ we get that $0 < q := a^2 + 7b^2 \equiv b^2(x_0^2 + 7) \equiv 0 \pmod p$. But, $q = a^2 + 7b^2 \leq m^2 + 7m^2 = 8m^2 < 8p$. It follows that $q \in \{p, 2p, 3p, 4p, 5p, 6p, 7p\}$. We need to eliminate the cases

$q \in \{2p, 3p, 4p, 5p, 6p, 7p\}$. If $q = 7p$ then $7p = a^2 + 7b^2$ which implies that a is a multiple of 7, or $a = 7a'$, which gives $p = b^2 + 7a'^2$ as wanted.

If $q = 3p$, then $q = 3(14k' + r) = 7\ell + s$ where $s \in \{3, 5, 6\}$. But this is impossible because $q \equiv a^2 \pmod 7$. The same argument works if $q = 6p$, because $r' \in \{1, 2, 4\}$ if and only if $6r' \in \{3, 5, 6\} \pmod 7$. Similarly, the case $p = 5p$ is no difference.

If $q = 2p$ or $a^2 + 7b^2 = 2p$ implies that a and b cannot be both odd, since in this case $a^2 + 7b^2$ is a multiple of 8 and $2p$ is not. Therefore a and b must be both even, but that shows that $2p$ is a multiple of 4. Again this is not the case.

Finally, if $q = 4p$ then the argument above works the same way but in the end we just simplify by a 4.

3. Cases $q \in \{11, 17, 19\}$

Given a big prime p, the characterizations in Theorem 1.4 cannot be easily checked. Instead, one can show a similar result that is slightly less but in the same spirit of Theorem 1.1.

Theorem 3.1. *(i) A prime $p > 17$ is of the form $a^2 + 17b^2$ or $2p = a^2 + 17b^2$, for some $a, b \in \mathbb{N}$ if and only if $p \equiv (2j + 1)^2$ (mod 68) for some $j = 0, ..., 7$.*

(ii) The representation of a prime as in part (a) is exclusive, i.e. a prime p cannot be of the form $a^2 + 17b^2$ and at the same time $2p = x^2 + 17y^2$, for some $x, y \in \mathbb{N}$.

Proof. (i)
" $\Rightarrow$ " If the prime p can be written $p = a^2 + 17b^2$ then $p \equiv a^2 \pmod{17}$ with a not divisible by 17. We observe that a and b cannot be both odd or both even. Then $p \equiv 1 \pmod 4$. If $p = 68k + r$ with $r \in \{0, 1, 2, ..., 67\}$ then $r \equiv 1 \pmod 4$, not a multiple of 17 and a quadratic residue modulo 17, i.e. $r = 17\ell + r'$ with $r' \in \{1, 2, 4, 8, 9, 13, 15, 16\}$. This gives $r \in \{1, 9, 13, 21, 25, 33, 49, 53\}$. One can check that these residues are covered in a one-to-one way by the odd squares j^2, $j \in \{1, 3, 5, 7, 9, 11, 13, 15\}$.

If $2p = a^2 + 17b^2$ then $2p \equiv a^2 \pmod{17}$ with a not divisible by 17. In this case a and b must be both odd and then $2p = a^2 + 17b^2 \equiv 2 \pmod 8$. This implies, as before, that $p \equiv 1 \pmod 4$. If $p = 68k + r$ with $r \in \{0, 1, 2, ..., 67\}$ then $r \equiv 1 \pmod 4$, not divisible by 17 and $2r$ is a quadratic residue modulo 17. Interestingly enough, we still have $r \in \{1, 9, 13, 21, 25, 33, 49, 53\}$.
" $\Leftarrow$ " We have $p \equiv j^2 \pmod{17}$ and so $(\frac{p}{17}) = 1$. By the Theorem 2.1, we have $(\frac{17}{p})(\frac{p}{17}) = (-1)^{8\frac{(p-1)}{2}} = 1$ which implies $(\frac{17}{p}) = 1$.

Since $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, we get that $(\frac{-17}{p}) = (-1)^{\frac{p-1}{2}}$. If $p = 68k + j^2$ with $j \in \{1, 3, 5, 7, 9, 11, 13, 15\}$, we see that $(\frac{-17}{p}) = 1$. Therefore $x^2 \equiv -17 \pmod{\text{p}}$ has a solution x_0. As in the case $q = 7$, if we use the same idea of the Pi Pigeonhole Principle we obtain that $q = a^2 + 17b^2 < 18p$ for some $a, b \in \mathbb{Z}$ and $q \equiv 0 \pmod{\text{p}}$. Hence $q = \ell p$ with $\ell \in \{1, 2, ..., 17\}$. We may assume that $gcd(a, b) = 1$, otherwise we can simplify the equality $q = \ell p$ by $gcd(a, b)$ which cannot be p. Clearly if $\ell = 1$, $\ell = 2$ or $\ell = 17$ we are done. Since $q \equiv 0$, 1 or 2 (mod 4) and $p \equiv 1 \pmod 4$ we cannot have $\ell \in \{3, 7, 11, 15\}$. If $\ell \in \{4, 8, 12, 16\}$, $\ell = 4\ell'$, we can simplify the equality by a

4 and reduce this case to $\ell' \in \{1,2,3,4\}$. Each one of these situations leads to either the conclusion of our claim or it can be excluded as before or reduced again by a 4.

(Case $\ell = 5$ or $\ell = 10$) Hence $q = \ell p = a^2 + 17b^2 \equiv a^2 + 2b^2 \equiv 0 \pmod 5$. If b is not a multiple of 5 then this implies $x^2 \equiv -2 \pmod 5$ which is not true. Hence b must be a multiple of 5 and then so must be a. Then the equality $\ell p = a^2 + 17b^2$ implies that ℓp is a multiple of 25 which is not possible.

(Case $\ell = 6$ or $\ell = 14$) In this case we must have a and b odd and then $q = 2(4s+1) = \ell p$ which is not possible.

(Case $\ell = 13$) In this case $4q = (2a)^2 + 17(2b)^2 = 2p(3^2 + 17(1)^2)$. We will use Euler's argument ([6], Lemma 1.4, p. 10) here. If we calculate $M = (2b)^2[3^2 + 17(1)^2] - 4q = [3(2b) - 2a][3(2b) + 2a]$, we see that 2(13) divides M and so it divides either $3(2b) - 2a$ or $3(2b) + 2a$. Without loss of generality we may assume that 2(13) divides $3(2b) - 2a$. Hence, we can write $3(2b) - 2a = 2(13)d$ for some $d \in \mathbb{Z}$. Next, we calculate

$$2a + 17d = 3(2b) - 2(13)d + 17d = 3(2b) - 9d,$$

which implies that $2a + 17d = 3e$ for some $e \in \mathbb{Z}$. Also, from the above equality we get that $2b = e + 3d$. Then

$$2p(26) = 4q = (2a)^2 + 17(2b)^2 = (3e - 17d)^2 + 17(e + 3d)^2 = 26(e^2 + 17d^2) \Rightarrow$$
$$2p = e^2 + 17d^2.$$

(Case $\ell = 9$) We have $4q = (2a)^2 + 17(2b)^2 = 2p(1^2 + 17(1)^2)$. We calculate $M = (2b)^2[1^2 + 17(1)^2] - 4q = (2b - 2a)(2b + 2a)$, we see that 2(9) divides M and so it divides either $2b - 2a$ or $2b + 2a$. We need to look into two possibilities now. First 2(9) divides one of the factors $2b - 2a$ or $2b + 2a$, or 2(3) divides each one of them. In the second situation we can see that 3 divides $4a = 2b + 2a - (2b - 2a)$ and so 3 must divide b too. This last possibility is excluded by the assumption that $gcd(a, b) = 1$. Without loss of generality we may assume that 2(9) divides $2b - 2a$. Hence, we can write $2b - 2a = 2(9)d$ for some $d \in \mathbb{Z}$. We set, $2a = e - 17d$ and observe that $2b = 2a + 18d = e - 17d + 18d = e + d$. Then

$$2p(18) = 4q = (2a)^2 + 17(2b)^2 = (e - 17d)^2 + 17(e + d)^2 = 18(e^2 + 17d^2) \Rightarrow$$
$$2p = e^2 + 17d^2.$$

(ii) To show this claim, we may use Euler's argument as above. □

For primes q which are multiples of four minus one, the patterns suggest that we have to change the modulo but also there are more trickier changes. Let us look at the cases $q = 11$ and $q = 19$. In case $q = 11$, we have seen that the quadratic form $a^2 + 11b^2$ in Theorem 1.1 can be separated by a polynomial from the other possible forms of representing primes which are quadratic residues of odd numbers modulo 22.

Theorem 3.2. *(i) A prime $p > 11$ is of the form $a^2 + 11b^2$ or $3p = a^2 + 11b^2$, for some $a, b \in \mathbb{N}$ if and only if $p \equiv (2j+1)^2$ (mod 22) for some $j = 0, ..., 4$.*

(ii) A prime $p > 19$ satisfies $4p = a^2 + 19b^2$, for some $a, b \in \mathbb{N}$ if and only if $p \equiv (2j+1)^2$ (mod 38) for some $j = 0, ..., 8$.

(iii) The representations of a prime as in part (i) are exclusive, i.e. a prime p cannot be in both representations.

We leave these proofs for the interested reader.

4. Proof of Theorem 1.6

Clearly the inclusions $A \cap B \subset C$ and $C \cap A \subset B$ are covered by Proposition 1.5. To show $B \cap C \subset A$ we will first prove it for $t = 2p$ with p a prime. Since $2p = a^2 + b^2$ we have $a^2 \equiv -b^2 \pmod{p}$. Because $p > 2$, a cannot be divisible by p and so it has an inverse (mod p) say a^{-1}. This shows that $x_0 = ba^{-1}$ is a solution of the equation $x^2 \equiv -1 \pmod{p}$. Similarly since $2p = 2(x^2 - xy + y^2)$ we get that $4(x^2 - xy + y^2) = (2x - y)^2 + 3y^2 \equiv 0 \pmod{p}$. This gives a solution y_0 of the equation $x^2 \equiv -3 \pmod{p}$. So, we have $z_0 = x_0 y_0$ satisfying $z_0^2 \equiv 3 \pmod{p}$. Let us now apply the Pigeonhole Principle as before: we let $m \in \mathbb{N}$ be in such a way that $m^2 < p < (m+1)^2$. We consider the function $g : \{0, 1, 2, ..., m\} \times \{0, 1, 2, ..., m\} \to \{0, 1, 2, ..., p-1\}$ defined by $g(u, v) \equiv u + vz_0 \pmod{p}$. Since $(m+1)^2 > p$, we must have two distinct pairs (a'', b'') and (a', b') such that $g(a'', b'') = g(a', b')$. Then $a'' - a' \equiv (b' - b'')z_0 \pmod{p}$. Then, if we let $r = a'' - a'$, and $s = b' - b''$ we get that $q := r^2 - 3s^2 \equiv s^2(z_0^2 - 3) \equiv 0 \pmod{p}$. So, q needs to be a multiple of p. If $q = 0$ then $r = \pm s\sqrt{3}$ which is not possible because r and s are integers not both equal to zero. If $q > 0$ then $0 < q \leq r^2 < p$, which is again impossible. It remains that $q < 0$, and so $0 < -q = 3s^2 - r^2 \leq 3s^2 < 3p$. This leaves only two possibilities for q: either $q = -p$ or $q = -2p$. Hence, we need to exclude the case $3s^2 - r^2 = p$. This implies $4p = 12s^2 - 4r^2 = (2x - y)^2 + 3y^2$. Then $4r^2 + (2x - y)^2 \equiv 0 \pmod{3}$. Since -1 is not a quadratic residue modulo 3 we must have r divisible by 3 which is gives $p = 3$ but we cannot have $6 = a^2 + b^2$. It remains that $2p = 3s^2 - r^2$. Let us observe that in this case s and r cannot be both even or of different parities since p must be of the form $4k + 1$. Hence, we have the representation $p = (\frac{3s+r}{2})^2 - 3(\frac{s+r}{2})^2$.

To prove the inclusion in general we just need to observe that for any number $t \in B \cap C$ and a prime $p > 2$ dividing t, then if p is of the form $4k + 3$ then it divides a and b and so p^2 divides t. The same is true if p is of the form $6k - 1$. Clearly all the primes that appear in the decomposition of t to an even power they can be factored out and reduce the problem to factors of the form $12k + 1$ but for these factors we can apply the above argument and use the identities:

$$(y^2 - 3x^2)(v^2 - 3u^2) = (3ux + vy)^2 - 3(xv + uy)^2,$$
$$2(x^2 - 3y^2) = 3(x + y)^2 - (x + 3y)^2.$$

References

[1] Barrucand, P., Cohn, H., *Note on primes of type x^2+32y^2, class number and residuacity*, J. Reine Angew. Math., **238**(1969), 67-70.

[2] Brink, D., *Five peculiar theorems on simultaneous representation of primes by quadratic forms*, J. Number Theory, **129**(2009), no. 2, 464-468.

[3] Chandler, R., Ionascu, E.J., *A characterization of all equilateral triangles in $\mathbb{Z}^3$*, Integers, Art. A19, **8**(2008).

[4] Cohn, H., *A course in computational algebraic number theory*, Springer, 1996.

[5] Cohn, H., *Advanced Topics in Computational Number Theory*, Springer, 1999.

[6] Cox, D.A., *Primes of the Form* $x^2 + ny^2$, Wiley-Interscience, 1989.

[7] Hudson, R.H., Williams, K.S., *Representation of primes by the principal form of the discriminant* $-D$ *when the classnumber* $h(-D)$ *is* 3, Acta Arithmetica, **57**(1991), 131-153.

[8] Ionascu, E.J., *A parametrization of equilateral triangles having integer coordinates*, Journal of Integer Sequences, **10**(2007).

[9] Ionascu, E.J., *A characterization of regular tetrahedra in* $\mathbb{Z}^3$, J. Number Theory, **129**(2009), 1066-1074.

[10] Ionascu, E.J., *Regular octahedrons in* $\{0, 1, ..., n\}^3$, Fasc. Math., **48**(2012), 49-59.

[11] Ionascu, E.J., Obando, R., *Cubes in* $\{0, 1, ..., n\}^3$, Integers, Art A9, **12A**(2012).

[12] Ionascu, E.J., Markov, A., *Platonic solids in* $\mathbb{Z}^3$, J. Number Theory, **131**(2011), no. 1, 138-145.

[13] Jackson, T., *A short proof that every prime* $p \equiv 3$ *(mod 8) is of the form* $x^2 + 2y^2$, *Amer. Math. Monthly*, **107**(2000), p. 447.

[14] Kaplansky, I., *The forms* $x^2 + 32y^2$ *and* $x^2 + 64y^2$, Proceedings of the American Mathematical Society, **131**(2003), no. 7, 2299-2300.

[15] Lemmermeyer, F., *Reciprocity Laws: from Euler to Eisenstein*, Berlin, Springer-Verlag, 2000.

[16] McDonald, I.G., *Regular simplexes with integer vertices*, C. R. Math. Rep. Acad. Sci. Canada, **9**(1987), No. 4, 189-193.

[17] Niven, I., Zuckerman, H.S., Montgomery, H.L., *An Introduction to the Theory of Numbers*, Fifth Edition, John Wiley & Sons, Inc., 1991.

[18] Rosen, K.H., *Elementary Number Theory and its Applications*, Fifth Edition, Addison Wesley, 2005.

[19] Spearman, B.K., Williams, K.S., *Representing primes by binary quadratic forms*, Amer. Math. Monthly, **99**(1992), 423-426.

[20] Schoenberg, I.J., *Regular Simplices and Quadratic Forms*, J. London Math. Soc., **12**(1937), 48-55.

[21] Uspensky, J.V., *On Jacobi's Arithmetical Theorems Concerning the Simultaneous Representation of Numbers by Two Different Quadratic Forms*, Transactions of the American Mathematical Society, **30**(1928), No. 2, 385-404.

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

Eugen J. Ionascu and Jeff Patterson
Department of Mathematics
Columbus State University
4225 University Avenue
Columbus, GA 31907
e-mail: `math@ejonascu.edu, j3phr3y@gmail.com`