PRIMES OF THE FORM $a^2 + qb^2$

EUGEN J. IONASCU AND JEFF PATTERSON

Abstract. In this paper we bring into attention an old subject in number theory. Fermat showed that a prime can be written as a sum of two squares if and only if it is a multiple of four plus one and the decomposition is unique. We are going to look into similar writings of primes as a sum of a square and a multiple of another square. We use elementary methods to show characterizations for similar representations.

1. INTRODUCTION

In [4], David Cox begins his book on the subject at hand with a very detailed introduction in the history of this subject and we definitely encourage the interested reader to consult his book. The methods employed are elementary at the beginning (mostly Chapter I) but quickly he dives into more advance mathematics such as Hilbert class filed theory, genus theory for field discriminants, elliptic functions and modular functions.

We arrived at this subject by studding the problem of finding all equilateral triangles in space with integer coordinates (see [3], [5], [7], and [8]). 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

$$a^2 + b^2 + c^2 = 3d^2 \tag{1}$$

for some integer d and side-lengths of the triangles are of the form $d\sqrt{2(m^2 - mn + n^2)}$ for some integers m and n. This leads to investigations of primes of the first three forms in the next theorem and also to representations of numbers by quadratic forms, such as $3d^2 - a^2$ or $3d^2 - 2b^2$, which are not positive definite forms. It is natural to ask whether or not the next prime forms in the Theorem 1.1 aren't related to similar parameterizations for regular simplices in $\mathbb{Z}^n$. In [14], Isaac Schoenberg gives a characterization of those n's for which such a simplex exists in $\mathbb{Z}^n$. Let us give the restatement of Schoenberg's result which appeared in [11]: *all n such that $n + 1$ is a sum of 1, 2, 4 or 8 squares.*

Also, we were wondering if elementary methods cannot be used to show more of the earlier results and how far can one go with that approach. We are just going to jump right to the point and give some of these facts. Some of them are classical and some were discovered by applying

Date: April 2^{nd}, 2012.
Key words and phrases. Quadratic Reciprocity, Pigeonhole principle.

these methods or by experimental investigations. Although we are not providing a proof here, we belived the statements in (xi) and (xix) in the next theorem, are new.

Theorem 1.1. *For an odd prime p we have $p = a^2 + qb^2$ for some integers a, b if and only if*

*(**i**) (Fermat) ($q = 1$) $p \equiv 1 \pmod 4$;*

*(**ii**) (Fermat) ($q = 2$) $p \equiv 1$ or $3 \pmod 8$;*

*(**iii**) (Fermat) ($q = 3$) $p = 3$ or $p \equiv 1 \pmod 6$;*

*(**iv**) ($q = 4$) $p \equiv 1 \pmod 4$;*

*(**v**) (Lagrange) ($q = 5$) $p = 5$ or $p \equiv 1$ or $3^2 \pmod{20}$;*

*(**vi**) ($q = 6$) $p \equiv 1$ or $7 \pmod{24}$;*

*(**vii**) ($q = 7$) $p = 7$ or $p \equiv j^2 \pmod{14}$ for some $j \in \{1, 3, 5\}$;*

*(**viii**) ($q = 8$) $p \equiv 1 \pmod 8$;*

*(**ix**) ($q = 9$) $p \equiv j^2 \pmod{36}$ for some $j \in \{1, 5, 7, 9\}$;*

*(**x**) ($q = 10$) $p \equiv j \pmod{40}$ for some $j \in \{1, 9, 11, 19\}$;*

*(**xi**) ($q = 11$) ($p > 11$) $p \equiv j^2 \pmod{22}$ for some $j \in \{1, 3, 5, 7, 9\}$ and the equation*

$$(x^3 - 3x)^2 + 11(x^2 - 1)^2 \equiv 0 \pmod p \quad \text{has a solution;}$$

*(**xii**) ($q = 12$) $p \equiv j \pmod{48}$ for some $j \in \{1, 13, 25, 37\}$;*

*(**xiii**) ($q = 13$) $p \equiv j^2 \pmod{52}$ for some $j \in \{1, 3, 5, 7, 9, 11\}$;*

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

$$x^2 \equiv -14 \text{ and } (x^2 + 1)^2 \equiv 8 \pmod p \text{ have solutions;}$$

*(**xv**) ($q = 15$) $p \equiv j \pmod{60}$ for some $j \in \{1, 19, 31, 49\}$;*

*(**xvi**) ($q = 16$) $p \equiv 1 \pmod 8$;*

*(**xvii**) ($q = 27$) $p \equiv 1 \pmod 3$ and the equation $x^3 \equiv 2 \pmod p$ has a solution;*

*(**xviii**) ($q = 31$) the equation*

$$(x^3 - 10x)^2 + 31(x^2 - 1)^2 \equiv 0 \pmod p \quad \text{has a solution;}$$

*(**xix**) ($q = 32$) $p \equiv 1 \pmod 8$ and the equation*

$$(x^2 - 1)^2 \equiv -1 \pmod p \text{ has a solution;}$$

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

As interesting corollaries of these equivalent 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 [15]), $\mathcal{P}_1 \subset \mathcal{P}_5$, $\mathcal{P}_{10} \subset \mathcal{P}_2$, ... 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 our statement in part (**xix**) of Theorem 1.1 implies this characterization because $x^8 + 4 = (x^4 - 2x^2 + 2)(x^4 + 2x^2 + 2)$ and clearly $(x^2 - 1)^2 + 1 = x^4 - 2x^2 + 2$. Also, another classical fact now is the interesting result is the Kaplansky's Theorem ([9]):

Theorem 1.2. *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 [4]). The uniqueness is understood in the sense that changes of sign, or rearrangements of x and y in case $q = 1$, are considered the same writing. It is clear that the Quadratic Reciprocity and higher order reciprocity results are useful ingredients here, and this is the only more sophisticated fact we will use here, but considered still part of elementary number theory.

Theorem 1.3. **[Gauss]** *For every p and q odd prime numbers we have*

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

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

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \ if \ the \ equation \ x^2 \equiv a \ (mod\ p) \ has \ a \ solution, \\ \\ -1 \ if \ the \ equation \ x^2 \equiv a \ (mod\ p) \ has \ no \ solution \end{cases} \tag{3}$$

2. Case **(vii)**

We are going to use some elementary ideas to show part (**vii**). We think this method can be used to prove all the statements except (xi), (xiv), and (xvii)-(xx). We learned about this technique from [12] and [13].

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 (mod 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 Theorem 1.3, we have $(\frac{7}{p})(\frac{p}{7}) = (-1)^{\frac{3(p-1)}{2}}$. Since $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, then

$$(\frac{-7}{p}) = (-1)^{\frac{p-1}{2}}(\frac{7}{p}) = (-1)^{\frac{p-1}{2}+\frac{3(p-1)}{2}}(\frac{p}{7}) = (\frac{r'}{7}),\ \text{where } p = 7(2k') + r', r' \in \{0, 1, .., 6\}.$$

This shows that if $r' \in \{1, 2, 4\}$ we have a solution x_0 for the equation $x^2 \equiv -7$ (mod 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 $g(u, v) \equiv u + vx_0$ (mod 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 $a'' - a' \equiv (b' - b'')x_0$ (mod p). Then, if we let $a = a'' - a'$, and $b = b' - b''$ we get that $0 < q := a^2 + 7b^2 \equiv b^2(x_0^2 + 7) \equiv 0$ (mod 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 $q \equiv a^2$ (mod 7). The same argument works if $q = 6p$, because $r' \in \{1, 2, 4\}$ if and only if $6r' \in \{3, 5, 6\}$ (mod 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 $q \in \{11, 17, 19\}$

Let us observe that the characterizations in Theorem 1.1 for the cases when one needs another polynomial of degree bigger than 2, are not easily checked for big primes p. Next we use still similar elementary methods to show the following result which seems to be the best what one can hope for in terms of a characterization in which certain quadratic forms of the form $a^2 = qb^2$ cannot be separated by simply the quadratic residues of odd numbers modulo $4q$.

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 1.3, 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 ([4], 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 reader.

References

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

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

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

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

[5] E. J. Ionascu, *A parametrization of equilateral triangles having integer coordinates*, Journal of Integer Sequences, Vol. **10**, 09.6.7. (2007)

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

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

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

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

[10] A. Markov, *Regular polytopes in* $\mathbb{Z}^n$, in progress

[11] I. G. McDonald, *Regular simplexes with integer vertices*, C. R. Math. Rep. Acad. Sci. Canada, Vol IX, No 4, 1987, pp. 189–193.

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

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

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

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

[16] 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) p. 144

Current address: Department of Mathematics, Columbus State University, 4225 University Avenue, Columbus, GA 31907

E-mail address: `math@ejonascu.edu`