

# involve

a journal of mathematics

The group of primitive almost pythagorean triples

Nikolai A. Krylov and Lindsay M. Kulzer



# The group of primitive almost pythagorean triples

Nikolai A. Krylov and Lindsay M. Kulzer

(Communicated by Scott Chapman)

We consider the triples of integer numbers that are solutions of the equation  $x^2 + qy^2 = z^2$ , where  $q$  is a fixed, square-free arbitrary positive integer. The set of equivalence classes of these triples forms an abelian group under the operation coming from complex multiplication. We investigate the algebraic structure of this group and describe all generators for each  $q \in \{2, 3, 5, 6\}$ . We also show that if the group has a generator with the third coordinate being a power of 2, such generator is unique up to multiplication by  $\pm 1$ .

## 1. Introduction and the group of PPTs

The set of pythagorean triples has various interesting structures. One of such structures is induced by a binary operation introduced by Taussky [1970]. Recall that a pythagorean triple (PT from now on) is an ordered triple  $(a, b, c)$  of natural numbers satisfying the identity  $a^2 + b^2 = c^2$ , and given two such triples  $(a_1, b_1, c_1)$  and  $(a_2, b_2, c_2)$  we can produce another one using

$$A := a_1a_2 + b_1b_2, \quad B := |a_1b_2 - a_2b_1|, \quad C := c_1c_2. \quad (1)$$

The natural relation  $(a, b, c) \simeq (\lambda a, \lambda b, \lambda c)$  for all  $\lambda \in \mathbb{N}$ , called projectivization, is an equivalence relation on this set. The operation mentioned above induces an abelian group structure on the set of equivalence classes of PTs where the identity element is the class of  $(1, 0, 1)$ . When  $a, b$  and  $c$  have no common prime divisors, the triple  $(a, b, c)$  is called *primitive*. It's easy to see that every equivalence class contains exactly one primitive pythagorean triple. Thus the set of all primitive pythagorean triples (PPTs from now on) forms an abelian group under the operation given in (1). The algebraic structure of this group, denoted by  $\mathbf{P}$ , was investigated by Eckert [1984], who proved that the group of PPTs is a free abelian group generated by all primitive triples  $(a, b, c)$ , where  $a > b$  and  $c$  is a prime number of the linear form  $c = 4n + 1$ . Every pythagorean triple  $(a, b, c)$  naturally gives a point on the unit circle with rational coordinates  $(a/c, b/c)$  and the equivalence class of PTs

---

MSC2010: 11D09, 20K20.

Keywords: pythagorean triples, infinitely generated commutative groups.

corresponds to a unique point on the circle. Operation (1) on the pythagorean triples corresponds to the “angle addition” of rational points on  $S^1$  and thus the group of PPTs is identified with the subgroup of all rational points on  $S^1$ . Analysis of this group was done by Tan [1996] and his Theorem 1 (p. 167) is equivalent to the proposition on page 25 of [Eckert 1984].

It is not hard to see that the composition law (1) naturally extends to the solutions of the Diophantine equation

$$X^2 + q \cdot Y^2 = Z^2 \tag{2}$$

where  $q$  is a fixed, square-free arbitrary positive integer. Via projectivization, we obtain a well defined binary operation on the set of equivalence classes of solutions to (2), and the set of such classes forms an abelian group as well. For some special values of  $q$ , including all  $q \in \{2, 3, 5, 6, 7, 15\}$ , such a group has been considered by Baldisserrri [1999]. However, it seems that the generators  $(3, 1, 4)$  for  $q = 7$ , and  $(1, 1, 4)$  for  $q = 15$ , are missing in [Baldisserrri 1999].

With the above in mind, we will consider in this paper the set of triples we call *almost pythagorean triples*, which are solutions to the equation (2). As in the case of PTs, each equivalence class here contains exactly one *primitive* almost pythagorean triple and therefore the set of equivalence classes is the set of *primitive almost pythagorean triples* (PAPTs).

In the next two sections we give a complete description of this group for  $q \in \{2, 3, 5, 6\}$ , similar to the one given in [Eckert 1984]. We also prove that for all  $q \neq 3$  the group of PAPTs is free abelian of infinite rank. In the last section we will discuss solutions  $(a, b, c)$  where  $c$  is even. Please note that some of the results we prove here have been obtained earlier by Baldisserrri; however, our proof of existence of elements of finite order is different from the one given in [Baldisserrri 1999]. We also explain that if  $(a, b, 2^k)$  is a nontrivial solution of (2) with  $q \neq 3$ , the set of all such solutions makes an infinite cyclic subgroup of the group of PAPTs. When  $q = 7$  and  $q = 15$  such a subgroup is missing in Theorem 2 of [Baldisserrri 1999].

## 2. Group of PAPTs

Let  $T_q$  denote the set of all integer triples  $(a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}$  such that  $a^2 + q \cdot b^2 = c^2$ . We introduce the following relation on  $T_q$ : two triples  $(a, b, c)$  and  $(A, B, C)$  are equivalent if there exist  $m, n \in \mathbb{Z} \setminus \{0\}$  such that  $m(a, b, c) = n(A, B, C)$ , where  $m(a, b, c) = (ma, mb, |mc|)$ . It is a straightforward check that this is an equivalence relation (also known as *projectivization*). We will denote the equivalence class of  $(a, b, c)$  by  $[a, b, c]$ . Note that  $[a, b, c] = [-a, -b, c]$ , but  $[a, b, c] \neq [-a, b, c]$ . We will denote the set of these equivalence classes by  $\mathcal{P}_q$ . Now we define a binary operation on  $\mathcal{P}_q$  that generalizes the one on the set of PPTs defined by (1).

**Definition 1.** For two arbitrary classes  $[a, b, c], [A, B, C] \in \mathcal{P}_q$ , define their sum by the formula

$$[a, b, c] + [A, B, C] := [aA - qbB, aB + bA, cC].$$

It is a routine check that this definition is independent of a particular choice of a triple and thus the binary operation is well defined. Here are two examples:

If  $q = 7$ ,

$$[3, 1, 4] + [3, 1, 4] + [3, 1, 4] = [3, 1, 4] + [2, 6, 16] = [-36, 20, 64] = [-9, 5, 16].$$

If  $q = 14$ ,

$$[5, 2, 9] + [13, 2, 15] = [9, 36, 135] = [1, 4, 15].$$

Since  $[a, b, c] + [1, 0, 1] = [a, b, c]$  and  $[a, b, c] + [-a, b, c] = [-a^2 - qb^2, 0, c^2] = [c^2, 0, c^2]$ , and the operation is associative (this check is left for the reader), we obtain the following result (compare [Baldisserrri 1999, Section 2] or [Weintraub 2008, Section 4.1]):

**Theorem 1.**  $(\mathcal{P}_q, +)$  is an abelian group. The identity element is  $[1, 0, 1]$  and the inverse of  $[a, b, c]$  is  $[a, -b, c] = [-a, b, c]$ .

The purpose of this paper is to see what the algebraic structure of  $(\mathcal{P}_q, +)$  is, and how it depends on  $q$ . From now on we will denote this group simply by  $\mathcal{P}_q$ . Please note that every equivalence class  $[a, b, c] \in \mathcal{P}_q$  can be represented uniquely by a primitive triple  $(\alpha, \beta, \gamma) \in T_q$ , where  $\alpha > 0$ . In particular, this gives us freedom to refer to primitive triples to describe elements of the group.

**Remark 1.** The group  $\mathcal{P}_q$  is a natural generalization of the group  $\mathbf{P}$  of PPTs. However,  $\mathcal{P}_1$  is not isomorphic to  $\mathbf{P}$ . The key point here is that the triple  $(0, 1, 1) \notin T_q$ , when  $q > 1$ , and the inverse of  $[a, b, c]$  is  $[a, -b, c] = [-a, b, c]$ . In particular, it forces the consideration of triples with  $a$  and  $b$  being all integers and not only positive ones. As a result, the triples  $(1, 0, 1)$  and  $(0, 1, 1)$  are not equivalent in  $T_1$ . In order for the binary operation on the set of PPTs to be well defined, the triple  $(0, 1, 1)$  must be equivalent to the identity triple  $(1, 0, 1)$  [Eckert 1984, (5), p. 23]. The relation between our group  $\mathcal{P}_1$  and the group  $\mathbf{P}$  of PPTs is given by the following direct sum decomposition:

$$\mathcal{P}_1 \cong \mathbf{P} \oplus \mathbb{Z}/2\mathbb{Z},$$

where the 2-torsion subgroup  $\mathbb{Z}/2\mathbb{Z}$  is generated by the element  $[0, 1, 1]$ . To prove this, one uses the map  $f : \mathbf{P} \oplus \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathcal{P}_1$  defined by

$$f((a, b, c), n) := \begin{cases} [a, b, c] + [1, 0, 1] = [a, b, c] & \text{if } n = 0, \\ [a, b, c] + [0, 1, 1] = [-b, a, c] & \text{if } n = 1. \end{cases}$$

It's easy to see that this  $f$  is an isomorphism.

**Remark 2.** The group  $\mathcal{P}_q$  also has a geometric interpretation: consider the set  $\mathcal{P}(\mathbb{Q})$  of all points  $(X, Y) \in \mathbb{Q} \times \mathbb{Q}$  that belong to the conic  $X^2 + qY^2 = 1$ . Let  $N = (1, 0)$  and take any two  $A, B \in \mathcal{P}(\mathbb{Q})$ . Draw the line through  $N$  parallel to the line  $(AB)$ ; then its second point of intersection with the conic  $X^2 + qY^2 = 1$  will be  $A + B$  (see [Lemmermeyer 2003b, Section 2.2; 2003a, Section 1] for the details). Via such geometric point of view, Lemmermeyer draws a close analogy between the groups  $\mathcal{P}(\mathbb{Z})$  of integral points on the conics in the affine plane and the groups  $E(\mathbb{Q})$  of rational points on elliptic curves in the projective plane. One of the key characteristics of  $\mathcal{P}(\mathbb{Z})$  and  $E(\mathbb{Q})$  is that both of the groups are finitely generated. Note however that if  $q > 0$ , the curve  $X^2 + qY^2 = 1$  has only two integer points,  $(\pm 1, 0)$ . One could consider the solutions of  $X^2 + qY^2 = 1$  over a finite field  $\mathbb{F}_q$  or over the  $p$ -adic numbers  $\mathbb{Z}_p$ . In each of these cases the group of all solutions is also finitely generated and we refer the reader to [Lemmermeyer 2003a, Section 4.2] for the exact formulas. In the present paper we investigate the group structure of all rational points on the conic  $X^2 + qY^2 = 1$  when  $q \geq 2$  and such group is never finitely generated, as we explain below.

### 3. Algebraic structure of $\mathcal{P}_q$

The classical enumeration of primitive pythagorean triples in the form

$$(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2) \text{ or } \left( \frac{u^2 - v^2}{2}, uv, \frac{u^2 + v^2}{2} \right)$$

is a useful component in understanding the group structure on the set of PPTs. We assume here that integers  $u$  and  $v$  have no common prime divisors; otherwise  $(a, b, c)$  won't be primitive. One could use the Diophantus chord method (see, for example, [Stillwell 2003, Section 1.7]) to derive such enumeration of all PPTs. This method can be generalized to enumerate all solutions to (2) for all square-free  $q > 1$ . In particular, if a primitive triple  $(a, b, c) \in T_q$ , then there exists a pair  $(u, v)$  of integers with no common prime divisors, such that

$$(a, b, c) = (\pm(u^2 - qv^2), 2uv, u^2 + qv^2) \text{ or } \left( \pm \frac{u^2 - qv^2}{2}, uv, \frac{u^2 + qv^2}{2} \right).$$

We can use this enumeration right away to prove that if  $c$  is prime, and  $(a, b, c) \in T_q$ , then such a pair of integers  $(a, b)$  is essentially unique. Here is the precise statement.

**Claim 1.** *If  $c$  is prime and*

$$x^2 + qy^2 = c^2 = a^2 + qb^2, \quad \text{where } abxy \neq 0,$$

*then  $(x, y) = (h_1a, h_2b)$ , where  $h_i = \pm 1$ .*

*Proof.* We apply Lemma 5.48 from Section 5.5 of [Weintraub 2008]. When  $2c = u^2 + qv^2$ , the proof needs an additional argument explaining why not just  $\beta/\alpha_0$  but also  $\beta/(2\alpha_0)$  will be in the ring of integers. It can be easily done considering separate cases of even and odd  $q$  and using the fact that if  $q$  is odd, then  $u$  and  $v$  used in the enumeration are both odd, and if  $q$  is even, then  $u$  will be even and  $v$  will be odd. We leave details to the reader.  $\square$

We will use these results when we discuss generators of  $\mathcal{P}_q$  below, but first we will find for which  $q > 1$  the group  $\mathcal{P}_q$  will have elements of finite order.

**3.1. Torsion in  $\mathcal{P}_q$ .** We follow Eckert's geometric argument [1984, p. 24] to understand the torsion of  $\mathcal{P}_q$ .

**Lemma 1.** *If  $q = 2$  or  $q > 3$ , then  $\mathcal{P}_q$  is torsion-free.  $\mathcal{P}_3 \cong \mathcal{F}_3 \oplus \mathbb{Z}/3\mathbb{Z}$ , where  $\mathcal{F}_3$  is a free abelian group.*

*Proof.* Let us assume that  $q \geq 2$ , and suppose the triple  $(a, b, c)$  is a solution of (2); that is, we can identify point  $(a/c, \sqrt{q} \cdot b/c)$  with  $e^{i\alpha}$  on the unit circle  $\mathbf{U}$ . Then a circle  $S_r^1$  with radius  $r = \alpha/(2\pi)$  is made to roll inside  $\mathbf{U}$  in the counterclockwise direction. The radius  $r$  is chosen this way so that the length of the circle  $S_r^1$  equals the length of the smaller arc of  $\mathbf{U}$  between the points  $e^{i\alpha}$  and  $e^0 = (1, 0)$ . Let us denote the point  $(1, 0)$  by  $P$  and assume that this point moves inside the unit disk when  $S_r^1$  rolls inside  $\mathbf{U}$ . When  $1 = kr$  for some positive integer  $k$ , this point  $P$  traces out a curve known as a hypocycloid. In this case the point  $P$  will mark off  $k - 1$  distinct points on  $\mathbf{U}$  and will return to its initial position  $(1, 0)$  so the hypocycloid will have exactly  $k$  cusps. If  $P$  doesn't return to  $(1, 0)$  after the first revolution around the origin, it might come back to  $(1, 0)$  after, say,  $n$  such revolutions. In that case  $n \cdot 2\pi = m \cdot \alpha$  for some  $m \in \mathbb{N}$ . Thus,  $\alpha$  is a rational multiple of  $\pi$ , or, to be more precise,

$$\alpha = \pi \cdot \frac{2n}{m}.$$

Due to Corollary 3.12 of [Niven 1956, Chapter 3, Section 5], in such a case the only possible rational values of  $\cos(\alpha)$  are  $0, \pm 1/2, \pm 1$ . Since  $\cos(\alpha) = a/c$ , where  $a \neq 0$ , we see that  $\mathcal{P}_q$  might have a torsion only if  $a/c = \pm 1/2$  or  $a/c = \pm 1$ . In the latter case we must have  $q \cdot b^2 = 0$ , which implies that the element  $[a, b, c]$  is the identity of  $\mathcal{P}_q$ . Suppose now  $a/c = \pm 1/2$ . Then  $qb^2 = 3a^2$  and if  $3 \neq q$  we will have a prime  $t \neq 3$  dividing  $q$ . We can assume without loss of generality that  $\gcd(a, b) = 1$ ; hence we obtain  $t \mid a$  and therefore  $t^2 \mid qb^2$ . Since  $q$  is square-free, we must have  $t \mid b^2$ , which contradicts that  $\gcd(a, b) = 1$ . Therefore if  $q = 2$  or  $q > 3$ ,  $\mathcal{P}_q$  is torsion-free. Suppose now  $q = 3$ . Then we obtain  $a = \pm b$  and we can multiply  $[a, b, c]$  by  $-1$ , if needed, to conclude that  $[a, b, c] = [1, 1, 2]$  or  $[a, b, c] = [1, -1, 2]$ . We have  $\langle [a, b, c] \rangle \cong \mathbb{Z}/3\mathbb{Z}$  in both these cases. This implies that  $\mathcal{P}_3/(\mathbb{Z}/3\mathbb{Z})$  is free abelian and hence  $\mathcal{P}_3 \cong \mathcal{F}_3 \oplus \mathbb{Z}/3\mathbb{Z}$ .  $\square$

**Remark 3.** There is another way to obtain this lemma via a different approach to the group  $\mathcal{P}_q$ ,  $q > 0$ . The authors are very thankful to Wladyslaw Narkiewicz who explained this alternative viewpoint to us (compare also with [Baldisserrri 1999]). Consider an imaginary quadratic field  $\mathbb{Q}(\sqrt{-q})$  and the multiplicative subgroup of nonzero elements whose norm is a square of a rational number. Let us denote this subgroup by  $\mathcal{A}_q$ . Obviously  $\mathbb{Q}^* \subset \mathcal{A}_q$  ( $\mathbb{Q}^*$  denotes the group of nonzero rational numbers). It is easy to see that  $\mathcal{P}_q \cong \mathcal{A}_q/\mathbb{Q}^*$ , and it follows from Theorem A of [Schenkman 1964] that  $\mathcal{A}_q$  is a direct product of cyclic groups. Hence the same holds for  $\mathcal{P}_q$ . If  $q = 1$  or  $q = 3$  the group  $\mathcal{A}_q$  will have elements of finite order since the field  $\mathbb{Q}(\sqrt{-q})$  has units different from  $\pm 1$ . These units will generate in  $\mathcal{P}_q$  the torsion factors  $\mathbb{Z}/2\mathbb{Z}$  or  $\mathbb{Z}/3\mathbb{Z}$ , when  $q = 1$  or  $q = 3$ , respectively.

**3.2. On generators of  $\mathcal{P}_q$  when  $q \leq 6$ .** In this subsection we assume that  $2 \leq q \leq 6$  and will describe the generators of  $\mathcal{P}_q$  similar to the way it was done in the proposition on pages 25 and 26 of [Eckert 1984]. We will use  $\mathcal{F}_q$  to denote the free subgroup of  $\mathcal{P}_q$ . As follows from Section 3.1 above,  $\mathcal{F}_q = \mathcal{P}_q$  for  $q \neq 3$ , and  $\mathcal{P}_3 \cong \mathcal{F}_3 \oplus (\mathbb{Z}/3\mathbb{Z})$ .

The key point in Eckert's description of the generators of the group of primitive pythagorean triples is the fact that a prime  $p$  can be a hypotenuse in a pythagorean triangle if and only if  $p \equiv 1 \pmod{4}$ . Our next lemma generalizes this fact to the cases of primitive triples from  $T_q$ , with  $q \in \{2, 3, 5, 6\}$ .

**Lemma 2.** *If  $(a, b, c) \in T_2$  is primitive and  $p$  is a prime divisor of  $c$ , then there exist  $u, v \in \mathbb{Z}$  such that  $p = u^2 + 2v^2$ . If  $(a, b, c) \in T_3$  is primitive and  $p$  is a prime divisor of  $c$ , then either  $p = 2$  or there exist  $u, v \in \mathbb{Z}$  such that  $p = u^2 + 3v^2$ . If  $(a, b, c) \in T_q$  is primitive where  $q = 5$  or  $q = 6$ , and  $p$  is a prime divisor of  $c$ , then there exist  $u, v \in \mathbb{Z}$  such that  $p = u^2 + qv^2$  or  $2p = u^2 + qv^2$ .*

*Proof.* Consider  $(a, b, c) \in T_q$ . Since  $a^2 + qb^2 = c^2$  where  $q \in \{2, 3, 5, 6\}$ , it follows from the generalized Diophantus chord method that there exist  $s, t \in \mathbb{Z}$  such that  $c = s^2 + qt^2$  or  $2c = s^2 + qt^2$ . Suppose  $c = p_1^{n_1} \cdots p_k^{n_k}$  is the prime decomposition of  $c$ .

Case 1:  $q = 2$ . We want to show that each prime  $p_i$  dividing  $c$  can be written in the form  $p_i = u^2 + 2v^2$  for some  $u, v \in \mathbb{Z}$  (note that if  $q$  is even,  $p_i \neq 2$ ). It is well known that a prime  $p$  can be written in the form

$$p = u^2 + 2v^2 \iff p = 8n + 1 \text{ or } p = 8n + 3 \quad \text{for some integer } n$$

(see [Stillwell 2003, Chapter 9] or [Cox 1989, Chapter 1]). Thus it's enough to show that if a prime  $p \mid c$  then  $p = 8n + 1$  or  $p = 8n + 3$ . Since  $p \mid c$ , and  $c = s^2 + qt^2$  or  $2c = s^2 + qt^2$ , we see that there exists  $m \in \mathbb{Z}$  such that  $pm = s^2 + 2t^2$  and hence  $-2t^2 \equiv s^2 \pmod{p}$ ; that is, the Legendre symbol  $\left(\frac{-2t^2}{p}\right)$  equals 1. Using basic

properties of the Legendre symbol, this implies that  $\left(\frac{-2}{p}\right) = 1$ . But  $\left(\frac{-2}{p}\right) = 1$  if and only if  $p = 8n + 1$  or  $p = 8n + 3$  as follows from the supplements to quadratic reciprocity law. This finishes the case with  $q = 2$ .

Case 2: Suppose now that  $q = 3$ . Then  $(1, 1, 2) \in T_3$  gives an example when  $c$  is divisible by prime  $p = 2$ . Note also that prime  $p = 2$  is of the form  $2p = u^2 + 3v^2$ . Assuming from now on that prime  $p$  dividing  $c$  is odd, we want to show that there exist  $u, v \in \mathbb{Z}$  such that  $p = u^2 + 3v^2$ , which is true if and only if there exists  $n \in \mathbb{Z}$  such that  $p = 3n + 1$  (again, see [Stillwell 2003] or [Cox 1989]). Hence, in our case, it suffices to show that if  $p \mid c$  then there exists  $n \in \mathbb{Z}$  such that  $p = 3n + 1$ . As in Case 1, there exists  $m \in \mathbb{Z}$  such that  $pm = s^2 + 3t^2$  for some  $s, t \in \mathbb{Z}$ . Therefore, we have that the Legendre symbol  $\left(\frac{-3}{p}\right) = 1$ , which holds if and only if  $p = 3n + 1$ . One can prove this using the quadratic reciprocity law (e.g., [Stillwell 2003, Section 6.8]).

Case 3: Suppose now that  $q = 5$ . Note that in this case  $c$  must be odd. Indeed, if  $c$  were even,  $x^2 + 5y^2$  would be divisible by 4, but on the other hand, since both of  $x$  and  $y$  must be odd when  $q$  is odd and  $c$  is even, we see that  $x^2 + 5y^2 \not\equiv 0 \pmod{4}$ . Since  $p \mid c$  then again there exists  $m \in \mathbb{Z}$  such that  $pm = s^2 + 5t^2$  for some  $s, t \in \mathbb{Z}$ ; that is,  $\left(\frac{-5}{p}\right) = 1$ . It is true that for any integer  $n$  and odd prime  $p$  not dividing  $n$  the Legendre symbol  $\left(\frac{-n}{p}\right) = 1$  if and only if  $p$  is represented by a primitive form  $ax^2 + bxy + cy^2$  of discriminant  $-4n$  such that  $a, b$ , and  $c$  are relatively prime [Cox 1989, Corollary 2.6]. Following an algorithm in Section 2.A of [Cox 1989] to show that every primitive quadratic form is equivalent to a reduced form one can show that the only two primitive reduced forms of discriminant  $-4 \cdot 5 = -20$  are  $x^2 + 5y^2$  and  $2x^2 + 2xy + 3y^2$ . Through a simple calculation it's easy to see that a prime  $p$  is of the form

$$p = 2x^2 + 2xy + 3y^2 \iff 2p = x^2 + 5y^2.$$

This finishes the third case.

Case 4: Lastly, let's consider the case when  $q = 6$ . Once again since  $p \neq 2$  and  $p \mid c$  then  $\left(\frac{-6}{p}\right) = 1$ . Using the same corollary used in Case 3, we see that  $p$  must be represented by a primitive quadratic form of discriminant  $-4 \cdot 6 = -24$ . Also, following the same algorithm used in Case 3 to determine such primitive reduced forms, we find that there are only two:  $x^2 + 6y^2$  and  $2x^2 + 3y^2$ . Through a simple calculation it can be determined that a prime  $p$  is of the form

$$p = 2x^2 + 3y^2 \iff 2p = x^2 + 6y^2.$$

Thus, the lemma is proven. □



**Remark 4.** One could write prime divisors from this lemma in a linear form if needed. It is a famous problem of classical number theory which primes can be expressed in the form  $x^2 + ny^2$ . The reader will find a complete solution of this problem in [Cox 1989]. For example, if  $p$  is prime, then for some  $n \in \mathbb{Z}$  we have

$$p = \begin{cases} 20n + 1, \\ 20n + 3, \\ 20n + 7, \\ 20n + 9, \end{cases}$$

if and only if  $p = x^2 + 5y^2$  or  $p = 2x^2 + 2xy + 3y^2$ . We refer the reader for the details to [Cox 1989, Chapter 1].

Now we are ready to describe all generators of  $\mathcal{P}_q$ , where  $q \in \{2, 3, 5, 6\}$ . Our proof is similar to the proof given by Eckert [1984], where he decomposes the hypotenuse of a right triangle into the product of primes and after that peels off one prime at a time, together with the corresponding sides of the right triangle. His description of prime  $p \equiv 1 \pmod{4}$  is equivalent to the statement that  $p$  can be written in the form  $p = u^2 + v^2$ , for some integers  $u$  and  $v$ , which is the case of Fermat's two square theorem. In the theorem below we also use quadratic forms for the primes.

**Theorem 2.** *Let us fix  $q \in \{2, 3, 5, 6\}$ . Then  $\mathcal{P}_q$  is generated by the set of all triples  $(a, b, p) \in T_q$  where  $a > 0$ , and  $p$  is prime such that there exist  $u, v \in \mathbb{Z}$  with  $p = u^2 + qv^2$ , or  $2p = u^2 + qv^2$ .*

*Proof.* Take arbitrary  $[r, s, d] \in \mathcal{P}_q$  and let us assume that  $(r, s, d) \in T_q$  will be the corresponding primitive triple with  $r > 0$ . Let  $d = p_1^{n_1} \cdots p_k^{n_k}$  be the prime decomposition of  $d$ . It is clear from what we've said above that  $d$  will be odd when  $[r, s, d] \in \mathcal{F}_q$ , and  $d$  will be even only if  $q = 3$  and  $[r, s, d] \notin \mathcal{F}_3$ . Our goal is to show that

$$[r, s, d] = \sum_{i=1}^k n_i \cdot [a_i, b_i, p_i],$$

where

$$a_i > 0, \quad n_i \cdot [a_i, b_i, p_i] := \underbrace{[a_i, b_i, p_i] + \cdots + [a_i, b_i, p_i]}_{n_i \text{ times}},$$

and  $p_i$  is either of the form  $u^2 + qv^2$  or of the form  $(u^2 + qv^2)/2$ . We deduce from Lemma 2 that each prime  $p_i \mid d$  can be written in one of these two forms. Hence, for all  $p_i$ , there exist  $a_i, b_i \in \mathbb{Z}$  such that  $a_i^2 + qb_i^2 = p_i^2$ . Indeed, if we have  $2p = u^2 + qv^2$ , then

$$4p^2 = (u^2 - qv^2)^2 + 4q(uv)^2$$

and since  $u^2 + qv^2$  is even,  $u^2 - qv^2$  will be even as well, and therefore we could write  $\alpha^2 + q\beta^2 = p^2$ , where  $\alpha = (u^2 - qv^2)/2$  and  $\beta = uv$ . Thus  $[a_i, b_i, p_i] \in \mathcal{P}_q$ . Since  $\mathcal{P}_q$  is a group, the equations

$$[r, s, d] = \begin{cases} [X_1, Y_1, D_1] + [a_k, b_k, p_k], \\ [X_2, Y_2, D_2] + [-a_k, b_k, p_k] \end{cases}$$

always have a solution with  $(X_i, Y_i, D_i) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}$ . The key observation now is that only one of the triples  $(X_i, Y_i, D_i)$  will be equivalent to a primitive triple  $(x, y, d_1)$ , with  $d_1 < d$ . Indeed, we have  $[r, s, d] = [X, Y, D] \pm [a, b, p]$  or

$$[X, Y, D] = [r, s, d] \pm [-a, b, p] = \begin{cases} [-ra - qsb, rb - sa, dp], \\ [ra - qsb, rb + sa, dp]. \end{cases}$$

Since  $p \mid d$ , we have  $dp \equiv 0 \pmod{p^2}$  and hence it is enough to show that either  $ra + qsb \equiv rb - sa \equiv 0 \pmod{p^2}$ , or  $ra - qsb \equiv rb + sa \equiv 0 \pmod{p^2}$  (see lemma on page 24 of [Eckert 1984]). From the identity

$$(sa - rb)(sa + rb) = s^2a^2 - r^2b^2 = s^2(a^2 + qb^2) - b^2(r^2 + qs^2) \equiv 0 \pmod{p^2},$$

we deduce that either  $p$  divides each of  $sa - rb$  and  $sa + rb$ , or  $p^2$  divides exactly one of these two terms. In the first case  $p \mid 2sa$ , which is impossible if  $p$  is odd, since then either  $a^2 > p^2$  or  $(r, s, d)$  won't be primitive. If we assume  $p = 2$ , then, as we explained in Lemma 2,  $q = 3$  and therefore  $(a, b, p) = (1, 1, 2)$  so  $(ra - qsb, rb + sa, dp) = (r - 3s, r + s, 2d)$ . But  $r + s \equiv r - 3s \pmod{4}$  and if  $4 \mid r + s$  we can write  $(ra - qsb, rb + sa, 2d) = 4((r - 3s)/4, (r + s)/4, d_1)$ , where  $d_1 = d/2$ . If  $r + s \equiv 2 \pmod{4}$ , we will divide each element of the other triple by 4.

Thus we can assume from now on that  $p$  is an odd prime and that either  $p^2 \mid sa - rb$  or  $p^2 \mid sa + rb$ . Let us assume without loss of generality that  $sa - rb = kp^2$  for some  $k \in \mathbb{Z}$ . Since the triple  $(-ra - qsb, rb - sa, dp)$  is a solution of (2), and the last two elements are divisible by  $p^2$ , it is obvious that the first element must be divisible by  $p^2$  too, that is, that  $ra + qsb = tp^2$ . This implies that

$$[X, Y, D] = [-ra - qsb, rb - sa, dp] = [-t, -k, d_1],$$

where  $d_1 = d/p < d$ , which we wanted to show. The other case is solved similarly. Note that only one of the two triples will have all three elements divisible by 4, which means that only  $[a, b, p]$  or  $[-a, b, p]$  can be subtracted from the original element  $[r, s, d]$  in such a way that the result will be in the required form.

Thus we can “peel off” the triple  $[a_k, b_k, p_k]$  from the original one  $[r, s, d]$  ending up with the element  $[x, y, d_1]$ , where now  $d_1 < d$ . Note that we can always assume that  $a_k > 0$  by using either  $[a_k, b_k, p_k]$  or  $[-a_k, -b_k, p_k]$ . Then simply

keep peeling off until all prime divisors of  $d$  give the required presentation of the element  $[r, s, d]$  as a linear combination of the generators  $[a_i, b_i, p_i]$ .  $\square$

**Remark 5.** Since these primes are the generators of  $\mathcal{P}_q$  when  $q \in \{2, 3, 5, 6\}$  and each prime (with exception  $p = 2$  when  $q = 3$ ) generates an infinite cyclic subgroup, it is obvious that  $\mathcal{P}_q$  contains an infinite number of elements. The same holds for  $\mathcal{P}_q$  when  $q \geq 7$ . This can be shown through properties of Pell's equation  $c^2 - qb^2 = 1$  where  $q$  is a square-free positive integer different from 1. This equation can be rewritten as  $c^2 = 1^2 + qb^2$ , which is in fact Equation (2) with specific solutions  $(1, b, c)$ . It is a classical fact of number theory that this equation always has a nontrivial solution and, in result, has infinitely many solutions (see [Weintraub 2008, Section 4.2] or [Stillwell 2003, Section 5.9]).

Note that it is not obvious that Pell's equation has a nontrivial solution for arbitrary  $q$ . For example, the smallest solution of the equation

$$1^2 + 61b^2 = c^2 \quad \text{is} \quad b = 226, 153, 980, \quad c = 1, 766, 319, 049.$$

Let us observe that the equation  $a^2 + 61b^2 = c^2$ , where  $a$  is allowed to be any integer, has many solutions with "smaller" integer triples. Three examples are  $[3, 16, 125]$ ,  $[6, 7, 55]$ , and  $[10, 9, 71]$ .

**3.3. On generators of  $\mathcal{P}_q$  when  $q \geq 7$  and the triples  $(a, b, 2^k)$ .** It is interesting to see how the method of peeling off breaks down in specific cases of  $q$  for  $q \geq 7$ . Here are some examples of PAPT's  $(a, b, c) \in T_q$ , where  $c$  is divisible by a prime  $p$  but there exist no nontrivial pair  $r, s \in \mathbb{Z}$  such that  $(r, s, p) \in T_q$ .

The primitive triple  $(9, 1, 10) \in T_{19}$  is a solution, where 10 is divisible by primes 2 and 5; however, it is impossible to find nonzero  $a, b \in \mathbb{Z}$  such that  $a^2 + 19b^2 = 5^2$ .

The primitive triple  $(3, 1, 4) \in T_7$  is a solution, where 4 is divisible by prime 2, however, it is impossible to solve  $a^2 + 7b^2 = 2^2$  in integers. In  $T_{15}$  the primitive triple  $(1, 1, 4)$  is a problematic solution for the same reason.

Baldisserri [1999, Observation 2, p. 304] mentions that if a nontrivial and primitive  $(a, b, c)$  solves (2), then  $c$  can be even only when  $q \equiv 3 \pmod{4}$ . Moreover, if  $q \equiv 3 \pmod{8}$ , we must have  $c = 2 \cdot \text{odd}$ , but if  $q \equiv 7 \pmod{8}$  we can have  $c$  divisible by any power of 2. Indeed, as we just mentioned above, the triple  $(3, 1, 4)$  solves (2) with  $q = 7$ , and clearly can not be presented as a sum of two "smaller" triples. Since  $\mathcal{P}_7$  is free, we see that  $(3, 1, 4)$  must generate a copy of  $\mathbb{Z}$  inside  $\mathcal{P}_7$ , and one can easily check that we have

$$2 \cdot [3, 1, 4] = \pm [1, 3, 2^3], \quad 3 \cdot [3, 1, 4] = \pm [9, 5, 2^4], \quad 4 \cdot [3, 1, 4] = \pm [31, 3, 2^5], \quad \dots$$

The same holds for the triple  $(1, 1, 4) \in T_{15}$  but somehow these two generators of  $\mathcal{P}_7$  and  $\mathcal{P}_{15}$  are not mentioned in Theorem 2 of [Baldisserri 1999].

Can we have more than one such generator for a fixed  $q$ ? In other words, how many nonintersecting  $\mathbb{Z}$ -subgroups of  $\mathcal{P}_q$  can exist, provided that each subgroup is generated by a triple where  $c$  is a power of 2? The following theorem shows that there can be only one such generator (for the definition of *irreducible solution* we refer the reader to [Baldisserrri 1999, p. 304], but basically it means that this solution is a generator of the group of PAPT's).

**Theorem 3.** *Fix  $q$  as above and assume that the triple  $(a, b, 2^k)$  is an irreducible solution of (2). If  $(x, y, 2^r) \in T_q$  and  $r \geq k$ , then there exists  $n \in \mathbb{Z}$  such that*

$$[x, y, 2^r] = n \cdot [a, b, 2^k].$$

*Proof.* Our idea of the proof is to show that given such a triple  $(x, y, 2^r) \in T_q$  with  $r \geq k$ , we can always peel off (i.e., add or subtract) one copy of  $(a, b, 2^k)$  so the resulting primitive triple will have the third coordinate less than or equal to  $2^{r-1}$ . Thus we consider

$$[S, T, V] := [x, y, 2^r] \pm [a, b, 2^k] = \begin{cases} [xa - qyb, ay + xb, 2^{r+k}], \\ [xa + qyb, ay - xb, 2^{r+k}]. \end{cases}$$

Since  $a, b, x$  and  $y$  are all odd, either  $ay + xb$  or  $ay - xb$  must be divisible by 4. Let's assume that  $4 \mid ay - xb$  and hence we can write  $ay - xb = 2^d \cdot R$ , where  $d \geq 2$ . Clearly, it's enough to prove that  $d \geq k + 1$ . We prove it by induction; that is, we will show that if  $d \leq k$ , then  $R$  must be even.

Since  $S = xa + qyb$  we could write

$$\begin{pmatrix} 2^d \cdot R \\ S \end{pmatrix} = \begin{pmatrix} -b & a \\ a & qb \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{and hence} \quad \begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{2^{2k}} \cdot \begin{pmatrix} qb & -a \\ -a & -b \end{pmatrix} \cdot \begin{pmatrix} 2^d \cdot R \\ S \end{pmatrix},$$

which gives  $bS = -2^{2k}y - a2^dR$ . Since  $(bS, bT, bV) \in T_q$ , we can also write

$$(2^{2k}y + a2^dR)^2 + qb^2 \cdot (2^dR)^2 = b^2 \cdot 2^{2r+2k}.$$

This last identity is equivalent to the following one (after using  $a^2 + qb^2 = 2^{2k}$  and dividing all terms by  $2^{2k}$ ):

$$2^{2k}y^2 + 2^{d+1}ayR + 2^{2d}R^2 = b^22^{2r}.$$

Furthermore, we can cancel  $2^{d+1}$  as well, because  $1 < d \leq k \leq r$ , and then we will obtain that

$$ayR = b^22^{2r-d-1} - 2^{d-1}R^2 - 2^{2k-d-1}y^2 = \text{even},$$

which finishes the proof since  $a$  and  $y$  are odd. □

**Remark 6.** Please note that if a primitive triple  $(a, b, 2 \cdot d) \in T_q$  for  $q \equiv 7 \pmod{8}$ , it is easy to show that  $d$  must be even (compare with Observation 2 of [Baldisserrri 1999], where  $\lambda$  must be at least 2). When  $q \in \{7, 15\}$ , we obtain the

generators  $(3, 1, 4)$  and  $(1, 1, 4)$ , respectively. However, if, for example  $q = 23$ , the primitive solution  $(a, b, c)$  where  $c$  is the smallest power of 2 is  $(7, 3, 16)$  but  $(11, 1, 12)$  also belongs to  $\mathcal{P}_{23}$ .

### References

- [Baldisserri 1999] N. Baldisserri, “The group of primitive quasi-Pythagorean triples”, *Rend. Circ. Mat. Palermo* (2) **48**:2 (1999), 299–308. MR 2000g:11025 Zbl 0938.11014
- [Cox 1989] D. A. Cox, *Primes of the form  $x^2 + ny^2$ : Fermat, class field theory and complex multiplication*, John Wiley & Sons, New York, 1989. MR 90m:11016 Zbl 0701.11001
- [Eckert 1984] E. J. Eckert, “The group of primitive Pythagorean triangles”, *Math. Mag.* **57**:1 (1984), 22–27. MR 85a:51017 Zbl 0534.10010
- [Lemmermeyer 2003a] F. Lemmermeyer, “Conics: a poor man’s elliptic curves”, preprint, 2003. arXiv 0311306
- [Lemmermeyer 2003b] F. Lemmermeyer, “Higher descent on Pell conics, III: The first 2-descent”, preprint, 2003. arXiv 0311310
- [Niven 1956] I. Niven, *Irrational numbers*, Carus Mathematical Monographs **11**, Mathematical Association of America, 1956. MR 18,195c Zbl 0070.27101
- [Schenkman 1964] E. Schenkman, “On the multiplicative group of a field”, *Arch. Math. (Basel)* **15** (1964), 282–285. MR 30 #89 Zbl 0126.06801
- [Stillwell 2003] J. Stillwell, *Elements of number theory*, Springer, New York, 2003. MR 2004j:11001 Zbl 1112.11002
- [Tan 1996] L. Tan, “The group of rational points on the unit circle”, *Math. Mag.* **69**:3 (1996), 163–171. MR 1394795 Zbl 1044.11584
- [Tausky 1970] O. Tausky, “Sums of squares”, *Amer. Math. Monthly* **77** (1970), 805–830. MR 42 #3020 Zbl 0208.05202
- [Weintraub 2008] S. H. Weintraub, *Factorization: unique and otherwise*, Canadian Mathematical Society, Ottawa, ON, 2008. MR 2009b:11193 Zbl 1162.11003

Received: 2011-08-11

Revised: 2012-03-29

Accepted: 2012-04-29

nkrylov@siena.edu

*Department of Mathematics, Siena College,  
515 Loudon Road, Loudonville, NY 12211, United States*

lindsaykulzer@gmail.com

*Department of Mathematics, Siena College,  
515 Loudon Road, Loudonville, NY 12211, United States*

# involve

msp.org/involve

## EDITORS

### MANAGING EDITOR

Kenneth S. Berenhaut, Wake Forest University, USA, berenhks@wfu.edu

### BOARD OF EDITORS

Colin Adams	Williams College, USA colin.c.adams@williams.edu	David Larson	Texas A&M University, USA larson@math.tamu.edu
John V. Baxley	Wake Forest University, NC, USA baxley@wfu.edu	Suzanne Lenhart	University of Tennessee, USA lenhart@math.utk.edu
Arthur T. Benjamin	Harvey Mudd College, USA benjamin@hmc.edu	Chi-Kwong Li	College of William and Mary, USA ckli@math.wm.edu
Martin Bohner	Missouri U of Science and Technology, USA bohner@mst.edu	Robert B. Lund	Clemson University, USA lund@clemson.edu
Nigel Boston	University of Wisconsin, USA boston@math.wisc.edu	Gaven J. Martin	Massey University, New Zealand g.j.martin@massey.ac.nz
Amarjit S. Budhiraja	U of North Carolina, Chapel Hill, USA budhiraj@email.unc.edu	Mary Meyer	Colorado State University, USA meyer@stat.colostate.edu
Pietro Cerone	Victoria University, Australia pietro.cerone@vu.edu.au	Emil Minchev	Ruse, Bulgaria eminchev@hotmail.com
Scott Chapman	Sam Houston State University, USA scott.chapman@shsu.edu	Frank Morgan	Williams College, USA frank.morgan@williams.edu
Joshua N. Cooper	University of South Carolina, USA cooper@math.sc.edu	Mohammad Sal Moselehian	Ferdowsi University of Mashhad, Iran moslehian@ferdowsi.um.ac.ir
Jem N. Corcoran	University of Colorado, USA corcoran@colorado.edu	Zuhair Nashed	University of Central Florida, USA znashed@mail.ucf.edu
Toka Diagana	Howard University, USA tdiagana@howard.edu	Ken Ono	Emory University, USA ono@mathcs.emory.edu
Michael Dorff	Brigham Young University, USA mdorff@math.byu.edu	Timothy E. O'Brien	Loyola University Chicago, USA tobrie1@luc.edu
Sever S. Dragomir	Victoria University, Australia sever@matilda.vu.edu.au	Joseph O'Rourke	Smith College, USA orourke@cs.smith.edu
Behrouz Emamizadeh	The Petroleum Institute, UAE bemamizadeh@pi.ac.ae	Yuval Peres	Microsoft Research, USA peres@microsoft.com
Joel Foisy	SUNY Potsdam foisyjs@potsdam.edu	Y.-F. S. Pétermann	Université de Genève, Switzerland petermann@math.unige.ch
Errin W. Fulp	Wake Forest University, USA fulp@wfu.edu	Robert J. Plemmons	Wake Forest University, USA rjplemmons@wfu.edu
Joseph Gallian	University of Minnesota Duluth, USA jgallian@d.umn.edu	Carl B. Pomerance	Dartmouth College, USA carl.pomerance@dartmouth.edu
Stephan R. Garcia	Pomona College, USA stephan.garcia@pomona.edu	Vadim Ponomarenko	San Diego State University, USA vadim@sciences.sdsu.edu
Anant Godbole	East Tennessee State University, USA godbole@etsu.edu	Bjorn Poonen	UC Berkeley, USA poonen@math.berkeley.edu
Ron Gould	Emory University, USA rg@mathcs.emory.edu	James Propp	U Mass Lowell, USA jpropp@cs.uml.edu
Andrew Granville	Université Montréal, Canada andrew@dms.umontreal.ca	József H. Przytycki	George Washington University, USA przytyck@gwu.edu
Jerrold Griggs	University of South Carolina, USA griggs@math.sc.edu	Richard Rebarber	University of Nebraska, USA rrebarbe@math.unl.edu
Sat Gupta	U of North Carolina, Greensboro, USA sngupta@uncg.edu	Robert W. Robinson	University of Georgia, USA rwr@cs.uga.edu
Jim Haglund	University of Pennsylvania, USA jhaglund@math.upenn.edu	Filip Saidak	U of North Carolina, Greensboro, USA f_saidak@uncg.edu
Johnny Henderson	Baylor University, USA johnny_henderson@baylor.edu	James A. Sellers	Penn State University, USA sellersj@math.psu.edu
Jim Hoste	Pitzer College jhoste@pitzer.edu	Andrew J. Sterge	Honorary Editor andy@ajsterge.com
Natalia Hritonenko	Prairie View A&M University, USA nahritonenko@pvamu.edu	Ann Trenk	Wellesley College, USA atrenk@wellesley.edu
Glenn H. Hurlbert	Arizona State University, USA hurlbert@asu.edu	Ravi Vakil	Stanford University, USA vakil@math.stanford.edu
Charles R. Johnson	College of William and Mary, USA crjohnso@math.wm.edu	Antonia Vecchio	Consiglio Nazionale delle Ricerche, Italy antonia.vecchio@cnr.it
K. B. Kulasekera	Clemson University, USA kk@ces.clemson.edu	Ram U. Verma	University of Toledo, USA verma99@msn.com
Gerry Ladas	University of Rhode Island, USA gladas@math.uri.edu	John C. Wierman	Johns Hopkins University, USA wierman@jhu.edu
		Michael E. Zieve	University of Michigan, USA zieve@umich.edu

## PRODUCTION


Silvio Levy, Scientific Editor

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2013 is US \$105/year for the electronic version, and \$145/year (+\$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW<sup>®</sup> from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2013 Mathematical Sciences Publishers

# involve

2013

vol. 6

no. 1

Refined inertias of tree sign patterns of orders 2 and 3 D. D. OLESKY, MICHAEL F. REMPEL AND P. VAN DEN DRIESSCHE	1
The group of primitive almost pythagorean triples NIKOLAI A. KRYLOV AND LINDSAY M. KULZER	13
Properties of generalized derangement graphs HANNAH JACKSON, KATHRYN NYMAN AND LES REID	25
Rook polynomials in three and higher dimensions FERYAL ALAYONT AND NICHOLAS KRZYWONOS	35
New confidence intervals for the AR(1) parameter FEREBEE TUNNO AND ASHTON ERWIN	53
Knots in the canonical book representation of complete graphs DANA ROWLAND AND ANDREA POLITANO	65
On closed modular colorings of rooted trees BRYAN PHINEZY AND PING ZHANG	83
Iterations of quadratic polynomials over finite fields WILLIAM WORDEN	99
Positive solutions to singular third-order boundary value problems on purely discrete time scales COURTNEY DEHOET, CURTIS KUNKEL AND ASHLEY MARTIN	113



1944-4176(2013)6:1;1-A