



ELSEVIER

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



General Section

Pairing pythagorean pairs



Lorenz Halbeisen, Norbert Hungerbühler*

Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich,
Switzerland

ARTICLE INFO

Article history:

Received 20 January 2021

Received in revised form 16 June 2021

Accepted 12 July 2021

Available online 22 July 2021

Communicated by S.J. Miller

MSC:

11D72

11G05

Keywords:

Pythagorean pair

Elliptic curve

ABSTRACT

A pair (a, b) of positive integers is a *pythagorean pair* if $a^2 + b^2 = \square$ (i.e., $a^2 + b^2$ is a square). A pythagorean pair (a, b) is called a *double-pythapotent pair* if there is another pythagorean pair (k, l) such that (ak, bl) is a pythagorean pair, and it is called a *quadratic pythapotent pair* if there is another pythagorean pair (k, l) which is not a multiple of (a, b) , such that (a^2k, b^2l) is a pythagorean pair. To each pythagorean pair (a, b) we assign an elliptic curve $\Gamma_{a,b}$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, such that $\Gamma_{a,b}$ has positive rank over \mathbb{Q} if and only if (a, b) is a double-pythapotent pair. Similarly, to each pythagorean pair (a, b) we assign an elliptic curve Γ_{a^2,b^2} with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, such that Γ_{a^2,b^2} has positive rank over \mathbb{Q} if and only if (a, b) is a quadratic pythapotent pair. Moreover, in the later case we obtain that every elliptic curve Γ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is isomorphic to a curve of the form Γ_{a^2,b^2} , where (a, b) is a pythagorean pair. As a side-result we get that if (a, b) is a double-pythapotent pair, then there are infinitely many pythagorean pairs (k, l) , not multiples of each other, such that (ak, bl) is a pythagorean pair; the analogous result holds for quadratic pythapotent pairs.

© 2021 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

* Corresponding author.

E-mail addresses: lorenz.halbeisen@math.ethz.ch (L. Halbeisen), norbert.hungerbuehler@math.ethz.ch (N. Hungerbühler).

1. Introduction

A pair (a, b) of positive integers is a *pythagorean pair* if $a^2 + b^2$ is a square, denoted $a^2 + b^2 = \square$. A pythagorean pair (a, b) is called a *double-pythapotent pair* if there is another pythagorean pair (k, l) such that (ak, bl) is a pythagorean pair, *i.e.*,

$$a^2 + b^2 = \square, \quad k^2 + l^2 = \square, \quad \text{and} \quad (ak)^2 + (bl)^2 = \square.$$

Notice that for positive integers a, b , the sum $a^4 + b^4$ is never a square (see [7, Oeuvres, I, p. 327; III, p. 264], and hence (a^2, b^2) is never a pythagorean pair. Furthermore, a pythagorean pair (a, b) is called a *quadratic pythapotent pair* if there is another pythagorean pair (k, l) which is not a multiple of (a, b) , such that (a^2k, b^2l) is a pythagorean pair, *i.e.*,

$$a^2 + b^2 = \square, \quad k^2 + l^2 = \square, \quad \text{and} \quad (a^2k)^2 + (b^2l)^2 = \square.$$

To each pythagorean pair (a, b) we assign the elliptic curve

$$\Gamma_{a,b} : \quad y^2 = x^3 + (a^2 + b^2)x^2 + a^2b^2x$$

and show that the curve $\Gamma_{a,b}$ has torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and that (a, b) is a double-pythapotent pair if and only if $\Gamma_{a,b}$ has positive rank over \mathbb{Q} . With the points of infinite order on the curve $\Gamma_{a,b}$, we can generate infinitely many pythagorean pairs (k, l) , not multiples of each other, such that (ak, bl) are pythagorean pairs.

Similarly, for each pythagorean pair (a, b) , the elliptic curve

$$\Gamma_{a^2,b^2} : \quad y^2 = x^3 + (a^4 + b^4)x^2 + a^4b^4x$$

has torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and (a, b) is a quadratic pythapotent pair if and only if Γ_{a^2,b^2} has positive rank over \mathbb{Q} . Moreover, we can show that every elliptic curve Γ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is isomorphic to a curve of the form Γ_{a^2,b^2} for some pythagorean pair (a, b) . Similar as above, with the points of infinite order on the curve Γ_{a^2,b^2} , we can generate infinitely many pythagorean pairs (k, l) , not multiples of each other, such that (a^2k, b^2l) are pythagorean pairs.

Remark 1. In a landmark article, Heegner [6] discovered the deep and far-reaching connection between congruent numbers and elliptic curves: A given number is congruent if and only if a certain elliptic curve has positive rank over \mathbb{Q} . More precisely, to any positive integer A , the elliptic curve

$$\Gamma_A : \quad y^2 = x^3 - A^2x$$

with torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is associated, and A is a congruent number if and only if Γ_A has positive rank over \mathbb{Q} . Moreover, with the points of infinite

order on the curve Γ_A , one can generate infinitely many rational triples (r, s, t) such that $r^2 + s^2 = t^2$ and $\frac{rs}{2} = A$ (an elementary proof of this result is given in [2]). It became a common theme to relate properties of pythagorean or heronian triples with elliptic curves and to use their arithmetic to gain insight in the diophantine solutions of the problem (see also [3]). Since the pair of squares (a^2, b^2) of a pythagorean pair (a, b) is never a pythagorean pair, it was natural to ask whether the Hadamard-Schur products (ak, bl) or (a^2k, b^2l) of two pairs $(a, b), (k, l)$ of pythagorean pairs can be a pythagorean pair or not. These questions lead, indeed, again in a natural way to associated elliptic curves of positive rank over \mathbb{Q} .

Examples. We give some examples of double-pythapotent pairs and of quadratic pythapotent pairs.

1. For $m = 5$ and $n = 2$, let $a = m^2 - n^2$ and $b = 2mn$. Then $(a, b) = (21, 20)$ is a pythagorean pair. Furthermore, let $k = 96$ and let $l = 110$. Then $96^2 + 110^2 = 146^2$ and

$$(21 \cdot 96)^2 + (20 \cdot 110)^2 = 2984^2$$

which shows that $(21, 20)$ is a double-pythapotent pair.

2. Let a, b as above and let $k = 805$ and $l = 6588$. Then $805^2 + 6588^2 = 6637^2$ and

$$(21^2 \cdot 805)^2 + (20^2 \cdot 6588)^2 = 2659005^2$$

which shows that $(21, 20)$ is also a quadratic pythapotent pair. However, as the following examples show, it is not the case that double-pythapotent pairs are also quadratic pythapotent pairs, or vice versa.

3. For $m = 4$ and $n = 3$, let $a = m^2 - n^2$ and $b = 2mn$. Then $(a, b) = (7, 24)$ is a pythagorean pair. Furthermore, let $k = 320$ and $l = 462$. Then $320^2 + 462^2 = 562^2$ and

$$(7 \cdot 320)^2 + (24 \cdot 462)^2 = 11312^2$$

which shows that $(7, 24)$ is a double-pythapotent pair. On the other hand, since the rank of the elliptic curve $\Gamma_{7^2, 24^2}$ is 0, $(7, 24)$ is not a quadratic pythapotent pair.

4. For $m = 4$ and $n = 1$, let $a = m^2 - n^2$ and $b = 2mn$. Then $(a, b) = (15, 8)$ is a pythagorean pair. Furthermore, let $k = 608$ and $l = 594$. Then $608^2 + 594^2 = 850^2$ and

$$(15^2 \cdot 608)^2 + (8^2 \cdot 594)^2 = 141984^2$$

which shows that $(15, 8)$ is a quadratic pythapotent pair. On the other hand, since the rank of the elliptic curve $\Gamma_{15, 8}$ is 0, $(15, 8)$ is not a double-pythapotent pair.

Remark 2. We obtained our parametrization Γ_{a^2,b^2} for elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, where (a, b) is a pythagorean pair, by Schroeter’s construction of cubic curves with line involutions (see [4]). Other new parametrizations obtained by Schroeter’s construction for elliptic curves with torsion groups $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, and $\mathbb{Z}/14\mathbb{Z}$ can be found in [5]. Furthermore, the curves $\Gamma_{a,b}$, where (a, b) is a pythagorean pair, were obtained by replacing the 4th powers in the parametrization Γ_{a^2,b^2} by squares.

2. Quadratic pythapotent pairs

In this section we consider quadratic pythapotent pairs — this case is slightly easier than the case with double-pythapotent pairs. First we show that the curve Γ_{a^2,b^2} has torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, and then we show how we obtain pythagorean pairs (k, l) from a point on Γ_{a^2,b^2} whose x -coordinate is a square such that (a^2k, b^2l) is a pythagorean pair.

Proposition 1. *If (a, b) is a pythagorean pair, then the elliptic curve Γ_{a^2,b^2} has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Vice versa, if an elliptic curve Γ has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, then there exists a pythagorean pair (a, b) such that Γ is isomorphic to Γ_{a^2,b^2} .*

Proof. Kubert [8, p. 217] gives the following parametrization for elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ (see also Rabarison [9, 3.14]):

$$y^2 + (1 - c)xy - ey = x^3 - ex^2$$

for

$$\tau = \frac{\tilde{m}}{\tilde{n}}, \quad d = \frac{\tau(8\tau + 2)}{8\tau^2 - 1}, \quad c = \frac{(2d - 1)(d - 1)}{d}, \quad e = (2d - 1)(d - 1).$$

After a rational transformation we obtain the curve

$$y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x$$

with

$$\tilde{a} = 256\tilde{m}^4(2\tilde{m} + \tilde{n})^4 + (4\tilde{m}^2 - (2\tilde{m} + \tilde{n})^2)^4 \quad \text{and} \quad \tilde{b} = 256\tilde{m}^4\tilde{n}^4(2\tilde{m} + \tilde{n})^4(4\tilde{m} + \tilde{n})^4.$$

Let $m := \tilde{m}$ and $n := \frac{2\tilde{m} + \tilde{n}}{2}$. Then we obtain the curve

$$y^2 = x^3 + 2^8((2mn)^4 + (m^2 - n^2)^4)x^2 + 2^{16}((2mn)^4 \cdot (m^2 - n^2)^4)x,$$

which is, for $a := m^2 - n^2$ and $b := 2mn$, equivalent to the curve

$$\Gamma_{a^2,b^2} : y^2 = x^3 + (a^4 + b^4)x^2 + a^4b^4x.$$

Notice that by definition of a and b , (a, b) is a pythagorean pair.

For the other direction, recall that for every pythagorean pair (a, b) we find positive integers λ, m, n such that m and n are relatively prime and $\{a, b\} = \{\lambda(m^2 - n^2), \lambda(2mn)\}$. So, by the substitutions $\tilde{m} := m$ and $\tilde{n} := 2(n - m)$, we see that every elliptic curve Γ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is isomorphic to a curve of the form Γ_{a^2, b^2} for some pythagorean pair (a, b) . ■

Remark 3. Let $a := m^2 - n^2$ and $b := 2mn$. If we replace m and n by $\bar{m} := m + n$ and $\bar{n} := m - n$, respectively, even though we obtain another pythagorean pair (\bar{a}, \bar{b}) , the corresponding elliptic curves Γ_{a^2, b^2} and $\Gamma_{\bar{a}^2, \bar{b}^2}$ are equivalent.

Theorem 2. *The pythagorean pair (a, b) is a quadratic pythapotent pair if and only if the elliptic curve Γ_{a^2, b^2} has positive rank over \mathbb{Q} .*

In order to prove Theorem 2, we first transform the curve Γ_{a^2, b^2} to a another curve on which we carry out our calculations.

Lemma 3. *If x_2 is the x -coordinate of a rational point on Γ_{a^2, b^2} , then*

$$x_0 := \frac{a^2 b^2}{x_2}$$

is the x -coordinate of a rational point on the curve

$$y^2 x = a^2 b^2 + (a^4 + b^4)x + a^2 b^2 x^2.$$

Proof. We work with homogeneous coordinates (x, y, z) . Consider the following transformation:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ \frac{1}{a^2 b^2} & 0 & 0 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

The point (x, y, z) belongs to the homogenized curve Γ_{a^2, b^2} if and only if the point (X, Y, Z) belongs to the curve $Y^2 X = a^2 b^2 Z^3 + (a^4 + b^4) X Z^2 + a^2 b^2 X^2 Z$. Hence, by dehomogenizing, we obtain the curve $y^2 x = a^2 b^2 + (a^4 + b^4)x + a^2 b^2 x^2$, which is equivalent to Γ_{a^2, b^2} , where the rational point (x_2, y_2) belongs to Γ_{a^2, b^2} if and only if there is a rational y' such that (x_0, y') belongs to $y^2 x = a^2 b^2 + (a^4 + b^4)x + a^2 b^2 x^2$. ■

Let $x_0 = \frac{p^2}{q^2}$ be a rational square and assume that x_0 is the x -coordinate of a rational point on $y^2 x = a^2 b^2 + (a^4 + b^4)x + a^2 b^2 x^2$. Then, by dividing through x_0 and clearing square denominators we obtain

$$a^2 b^2 \cdot q^4 + (a^4 + b^4) \cdot p^2 \cdot q^2 + a^2 b^2 \cdot p^4 = \square,$$

and since

$$a^2b^2 \cdot q^4 + (a^4 + b^4) \cdot p^2 \cdot q^2 + a^2b^2 \cdot p^4 = (a^2q^2 + b^2p^2) \cdot (a^2p^2 + b^2q^2),$$

this is surely the case when

$$a^2q^2 + b^2p^2 = \square \quad \text{and} \quad a^2p^2 + b^2q^2 = \square. \tag{1}$$

Lemma 4. *Let $P = (x_1, y_1)$ be a rational point on Γ_{a^2, b^2} and let x_2 be the x -coordinate of the point $2 * P$. Then $x_0 := \frac{a^2b^2}{x_2} = \frac{p^2}{q^2}$, where p and q satisfy (1).*

Proof. By Silverman and Tate [10, p.27],

$$x_2 = \frac{(x_1^2 - B)^2}{(2y_1)^2} \quad \text{for } B := a^4b^4,$$

and therefore

$$x_0 = \frac{a^2b^2}{x_2} = \frac{a^2b^2(2y_1)^2}{(x_1^2 - B)^2} = \frac{a^2b^2(4x_1^3 + 4Ax_1^2 + 4Bx_1)}{(x_1^2 - B)^2} = \frac{p^2}{q^2} \quad \text{for } A := a^4 + b^4.$$

Now, for p and q (with $a = m^2 - n^2$ and $b = 2mn$) we obtain

$$a^2q^2 + b^2p^2 = a^2(a^4b^4 + 2b^4x_1 + x_1^2)^2 = \square$$

and

$$a^2p^2 + b^2q^2 = b^2(a^4b^4 + 2a^4x_1 + x_1^2)^2 = \square$$

which completes the proof. ■

The next result gives a relation between rational points on Γ_{a^2, b^2} with square x -coordinates and pythagorean pairs (k, l) such that (a^2k, b^2l) is a pythagorean pair.

Lemma 5. *Every pythagorean pair (k, l) such that (a^2k, b^2l) is a pythagorean pair corresponds to a rational point on Γ_{a^2, b^2} whose x -coordinate is a square, and vice versa.*

Proof. Let $x_2 = \square$ be the x -coordinate of a rational point on Γ_{a^2, b^2} . Then, by Lemma 4, $\frac{a^2b^2}{x_2} = \frac{p^2}{q^2}$, where p and q satisfy (1), i.e., $a^2q^2 + b^2p^2 = \square$. So, $\frac{a^2}{b^2} + \frac{p^2}{q^2} = \rho^2$ for some $\rho \in \mathbb{Q}$. In other words, we have

$$\left(\frac{a}{b}\right)^2 + \left(\frac{p}{q}\right)^2 = \rho^2,$$

which implies that

$$\frac{a}{b} = \frac{2\rho t}{t^2 + 1} \quad \text{and} \quad \frac{p}{q} = \frac{\rho(t^2 - 1)}{t^2 + 1} \quad \text{for some } t \in \mathbb{Q}.$$

In particular, we have

$$\rho = \frac{a \cdot (t^2 + 1)}{b \cdot (2t)}.$$

Now, since $a^2p^2 + b^2q^2 = \square$, we have $(\frac{a}{b})^2 + (\frac{q}{p})^2 = \square$, hence, $\frac{a^2}{b^2} + \frac{(t^2+1)^2}{\rho^2(t^2-1)^2} = \square$, which implies that

$$a^4 \cdot (t^2 - 1)^2 + b^4 \cdot (2t)^2 = \square.$$

For $t = \frac{r}{s}$, we obtain

$$\frac{a^4 \cdot (r^2 - s^2)^2}{s^4} + \frac{b^4 \cdot 4r^2}{s^2} = \square,$$

which implies that

$$a^4 \cdot (r^2 - s^2)^2 + b^4 \cdot (2rs)^2 = \square,$$

and for $k := r^2 - s^2$, $l := 2rs$, we finally obtain

$$(a^2k)^2 + (b^2l)^2 = \square \quad \text{where } k^2 + l^2 = \square,$$

which shows that (a, b) is a quadratic pythapotent pair.

Assume now that we find a pythagorean pair (k, l) such that (a^2k, b^2l) is a pythagorean pair. Without loss of generality we may assume that k and l are relatively prime. Thus, we find relatively prime positive integers r and s such that $k = r^2 - s^2$ and $l = 2rs$. With $t := \frac{r}{s}$, a , and b , we can compute p and q , and finally obtain a rational point on Γ_{a^2, b^2} whose x -coordinate is a square. ■

We are now ready for the

Proof of Theorem 2. For every rational point P on Γ_{a^2, b^2} whose x -coordinate is a square, let (k_P, l_P) be the corresponding pythagorean pair. By Lemma 5 it is enough to show that (k_P, l_P) is a multiple of (a, b) if and only if P is a torsion point. Notice that if P is a point of infinite order, then for every integer i , $2i * P$ is a rational point on Γ_{a^2, b^2} with square x -coordinate, and not all of the corresponding pythagorean pairs (k_{2i*P}, l_{2i*P}) can be multiples of (a, b) .

Let us consider the x -coordinates of the torsion points on the curve Γ_{a^2, b^2} . For simplicity, we consider the 16 torsion points on the equivalent curve

$$y^2 = \frac{a^2b^2}{x} + (a^4 + b^4) + a^2b^2x.$$

The two torsion points at infinity are $(0, 1, 0)$ (which is the neutral element of the group) and $(1, 0, 0)$ (which is a point of order 2). The other two points of order 2 are $(-\frac{a^2}{b^2}, 0)$ and $(-\frac{b^2}{a^2}, 0)$, and the two points of order 4 are $(1, \pm(a^2 + b^2))$. The x -coordinates of the other 10 torsion points are $\frac{m(m+n)}{n(m-n)}, \frac{n(m-n)}{m(m+n)}, -\frac{m(m-n)}{n(m+n)}, -\frac{n(m+n)}{m(m-n)}$, and -1 . Obviously, $-1, -\frac{a^2}{b^2}$, and $-\frac{b^2}{a^2}$ are not squares of rational numbers. Furthermore, 0 would lead to $p = 0, q = 1, t = 1, r = 1, s = 0, k = 1$ and $l = 0$, and therefore, (k, l) is not a pythagorean pair. If $\frac{m(m+n)}{n(m-n)} = \square$, then, by multiplying with $n^2(m-n)^2$, also $mn(m^2 - n^2) = \square$, which would imply that $A := mn(m^2 - n^2)$ is a congruent number with $A = \square$. But this is impossible, since otherwise 1 would be a congruent number, which is not the case (see also [7, Oeuvres, I, p. 340] or [11, p. 163] for an annotated version of Fermat’s proof). Similarly, one can show that also $\frac{n(m-n)}{m(m+n)}, -\frac{m(m-n)}{n(m+n)}$ and $-\frac{n(m+n)}{m(m-n)}$ cannot be squares. Thus, the only value of x -coordinates of torsion points on the curve Γ_{a^2, b^2} which is a square is $x = 1$. This leads to $k = 2b$ and $l = 2a$, i.e., to the pythagorean pair $(2b, 2a)$, which is a multiple of (a, b) — notice that for $c := a^2 + b^2, (2a^2b)^2 + (2ab^2)^2 = (2abc)^2$. ■

Corollary 6. *If (a, b) is a quadratic pythapotent pair, then there are infinitely many pythagorean pairs (k, l) , not multiples of each other, such that (ak, bl) is a pythagorean pair.*

Proof. By Theorem 2, there exists a point P on Γ_{a^2, b^2} of infinite order. Now, for every integer $i, 2i * P$ is a rational point on Γ_{a^2, b^2} with square x -coordinate, and each of the corresponding pythagorean pairs $(k_{2i * P}, l_{2i * P})$ can be a multiple of just finitely many other such pythagorean pair. Thus, there are infinitely many integers j , such that the pythagorean pairs $(k_{2j * P}, l_{2j * P})$ are not multiples of each other. ■

Algorithm 1. The following algorithm describes how to construct pythagorean pairs (k, l) from rational points on Γ_{a^2, b^2} of infinite order.

- Let P be a rational point on Γ_{a^2, b^2} of infinite order and let x_2 be the x -coordinate of $2 * P$.
- Let p and q be relatively prime positive integers such that

$$\frac{q}{p} = \frac{\sqrt{x_2}}{ab}.$$

- Let r and s be relatively prime positive integers such that

$$\frac{r}{s} = \frac{bp + \sqrt{a^2q^2 + b^2p^2}}{aq}.$$

- Let $k := r^2 - s^2$ and let $l := 2rs$.

Then (a^2k, b^2l) is a pythagorean pair.

Example. For $m = 17$ and $n = 1$, let $a = m^2 - n^2$ and $b = 2mn$. Then $(a, b) = (288, 34)$ is a pythagorean pair. Now, the curve Γ_{a^2, b^2} , with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, has rank 2 with generators

$$P = (248223744, 21013140234240) \quad \text{and} \quad P' = (2105708544, -199666455920640).$$

The x -coordinate of $2 * P$ is $\frac{845105135616}{543169}$ which leads to $(k, l) = (212993, 229824)$ with

$$(288^2 \cdot 212993)^2 + (34^2 \cdot 229824)^2 = 17668488960^2,$$

and x -coordinate of $2 * P'$ is $\frac{10707037334317433880576}{87206592371809}$ which leads to

$$(k', l') = (2698811183, 25868703744)$$

with

$$(288^2 \cdot 2698811183)^2 + (34^2 \cdot 25868703744)^2 = 225838818984960^2.$$

Of course, we can also start with any other rational point on $\Gamma_{288^2, 34^2}$, *e.g.*, we can start with the point $Q = P + P'$. The x -coordinate of $2 * Q$ is $\frac{40012254481826306304}{79121251225}$ which leads to

$$(k, l) = (81291365, 1581381012)$$

with

$$(288^2 \cdot 81291365)^2 + (34^2 \cdot 1581381012)^2 = 6986052964272^2.$$

3. Double-pythapotent pairs

Below we consider double-pythapotent pairs. As above, we first show that the curve $\Gamma_{a,b}$ has torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and then we show how we obtain pythagorean pairs (k, l) from a point on $\Gamma_{a,b}$ with square x -coordinate such that (ak, bl) is a pythagorean pair. Since the calculations are similar, we shall omit the details.

Proposition 7. *If (a, b) is a pythagorean pair, then the elliptic curve*

$$\Gamma_{a,b}: \quad y^2 = x^3 + (a^2 + b^2)x^2 + a^2b^2x$$

has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Proof. Kubert [8, p. 217] gives the following parametrization for elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$:

$$y^2 + xy - ey = x^3 - ex^2$$

for

$$e = v^2 - \frac{1}{16} \quad \text{where } v \neq 0, \pm \frac{1}{4}.$$

After a rational transformation we obtain the curve

$$y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x$$

with

$$\tilde{a} = 2 \cdot (16v^2 + 1) \quad \text{and} \quad \tilde{b} = (16v^2 - 1)^2.$$

For $v = \frac{p}{q}$, $a = m^2 - n^2$, $b = 2mn$, let $p := \frac{1}{8}(a - b)$ and $q := \frac{1}{2}(a + b)$. Then the curve $y^2 + xy - ey = x^3 - ex^2$ is equivalent to the curve

$$\Gamma_{a,b}: \quad y^2 = x^3 + (a^2 + b^2)x^2 + a^2b^2x. \quad \blacksquare$$

Remark 4. Notice that there are p and q which are not of the above form, which implies that there are curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ which are *not* equivalent to some curve $\Gamma_{a,b}$.

Theorem 8. *The pythagorean pair (a, b) is a double-pythapotent pair if and only if the elliptic curve $\Gamma_{a,b}$ has positive rank over \mathbb{Q} .*

In order to prove Theorem 8, we again transform the curve $\Gamma_{a,b}$ to a another curve on which we carry out our calculations.

Lemma 9. *If x_2 is the x -coordinate of a rational point on $\Gamma_{a,b}$, then*

$$x_0 := \frac{ab}{x_2}$$

is the x -coordinate of a rational point on the curve

$$y^2x = ab + (a^2 + b^2)x + abx^2.$$

Proof. We can just follow the proof of Lemma 3, using the transformation

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ \frac{1}{ab} & 0 & 0 \end{pmatrix}. \quad \blacksquare$$

Let $x_0 = \frac{p}{q}$ be the x -coordinate of a rational point on $y^2x = ab + (a^2 + b^2)x + abx^2$, where $q = \tilde{q}^2$ and $p = ab \cdot \tilde{p}^2$ for some integers \tilde{q}, \tilde{p} . Then

$$ab \cdot y^2 \cdot \frac{p}{q} = ab \cdot y^2 \cdot \frac{ab\tilde{p}^2}{\tilde{q}^2} = y^2 \cdot \left(\frac{ab \cdot \tilde{p}}{\tilde{q}}\right)^2 = \square.$$

Therefore,

$$ab \cdot \left(ab + (a^2 + b^2) \cdot \frac{p}{q} + ab \cdot \frac{p^2}{q^2}\right) = \square,$$

and by clearing square denominators we obtain

$$ab \cdot (aq + bp) \cdot (ap + bq) = \square,$$

which is surely the case when

$$a \cdot (aq + bp) = \square \quad \text{and} \quad b \cdot (ap + bq) = \square. \tag{2}$$

Lemma 10. *Let $P = (x_1, y_1)$ be a rational point on $\Gamma_{a,b}$ and let x_2 be the x -coordinate of the point $2 * P$. Then $x_0 := \frac{ab}{x_2} = \frac{p}{q}$, where $q = \tilde{q}^2$ and $p = ab \cdot \tilde{p}^2$ for some integers \tilde{q}, \tilde{p} and p and q satisfy (2).*

Proof. By Silverman and Tate [10, p. 27],

$$x_2 = \frac{(x_1^2 - B)^2}{(2y_1)^2} \quad \text{for } B := a^4b^4,$$

and therefore

$$x_0 = \frac{ab}{x_2} = \frac{ab(4x_1^3 + 4Ax_1^2 + 4Bx_1)}{(x_1^2 - B)^2} = \frac{p}{q} \quad \text{for } A := a^4 + b^4.$$

So, $q = \square$ and $p = ab \cdot \tilde{p}^2$ for some integer \tilde{p} .

Now, for $x_1 = \frac{u}{v}$ and $x_0 = \frac{p}{q}$ (with $a = m^2 - n^2$ and $b = 2mn$) we obtain

$$a \cdot (aq + bp) = \frac{1}{v^4} \left(a^2 \cdot (a^2b^2v^2 + u(u + 2b^2v)) \right)^2 = \square$$

and

$$b \cdot (ap + bq) = \frac{1}{v^4} \left(b^2 \cdot (a^2b^2v^2 + u(u + 2a^2v)) \right)^2 = \square$$

which completes the proof. ■

The next result gives a relation between rational points on $\Gamma_{a,b}$ with square x -coordinate and pythagorean pairs (k, l) such that (a^2k, b^2l) is a pythagorean pair.

Lemma 11. *Every pythagorean pair (k, l) such that (a^2k, b^2l) is a pythagorean pair corresponds to a rational point on $\Gamma_{a,b}$ whose x -coordinate is a square, and vice versa.*

Proof. Let $x_2 = \square$ be the x -coordinate of a rational point on $\Gamma_{a,b}$. Then, by Lemma 10, $\frac{ab}{x_2} = \frac{ab \cdot f^2}{g^2}$, where $p = ab \cdot f^2$ and $q = g^2$ satisfy (2), i.e., $a^2g^2 + a^2b^2f^2 = \square$. So, $(\frac{q}{f})^2 + b^2 = \rho^2$ for some $\rho \in \mathbb{Q}$ and $(\frac{q}{f})^2 + a^2 = \square$. Let $\frac{q}{f} = \frac{2\rho t}{t^2+1}$ and $b = \frac{\rho(t^2-1)}{t^2+1}$. Then $\rho = \frac{b(t^2+1)}{t^2-1}$ and $\frac{q}{f} = \frac{2bt}{t^2-1}$, which gives us

$$t = \frac{bf \pm \sqrt{g^2 + b^2f^2}}{g}.$$

Since

$$g^2 + b^2f^2 = q + \frac{b^2p}{ab} = q + \frac{bp}{a},$$

by multiplying with a^2 we get

$$a^2 \cdot (g^2 + b^2f^2) = a^2 \cdot q + ab \cdot p = a(aq + bp).$$

Hence, by Lemma 10, $g^2 + b^2f^2 = \square$ and therefore t is rational, say $t = \frac{r}{s}$. Finally, since $(\frac{q}{f})^2 + a^2 = \square$, we obtain

$$a^2 \cdot (r^2 - s^2)^2 + b^2 \cdot (2rs)^2 = \square,$$

and for $k := r^2 - s^2, l := 2rs$, we finally get

$$(ak)^2 + (bl)^2 = \square \quad \text{where } k^2 + l^2 = \square,$$

which shows that (a, b) is a double-pythapotent pair.

Assume now that we find a pythagorean pair (k, l) such that (ak, bl) is a pythagorean pair. Without loss of generality we may assume that k and l are relatively prime. Thus, we find relatively prime positive integers r and s such that $k = r^2 - s^2$ and $l = 2rs$. With $t := \frac{r}{s}, a$, and b , we can compute p and q , and finally obtain a rational point on $\Gamma_{a,b}$ whose x -coordinate is a square. ■

We are now ready for the

Proof of Theorem 8. For every rational point P on $\Gamma_{a,b}$ with square x -coordinate let (k_P, l_P) be the corresponding pythagorean pair. By Lemma 11 it is enough to show that no rational point with square x -coordinate has finite order.

Let us consider the x -coordinates of the torsion points on the curve $\Gamma_{a,b}$. For simplicity, we consider the 8 torsion points on the equivalent curve

$$y^2 = \frac{ab}{x} + (a^2 + b^2) + abx.$$

The two torsion points at infinity are $(0, 1, 0)$ (which is the neutral element of the group) and $(1, 0, 0)$ (which is a point of order 2). The other two points of order 2 are $(-\frac{a}{b}, 0)$ and $(-\frac{b}{a}, 0)$, and the four points of order 4 are $(1, \pm(a + b))$ and $(-1, \pm(a - b))$. Now, we have that none of the values

$$\frac{1}{ab}, \quad \frac{-1}{ab}, \quad \frac{-\frac{a}{b}}{ab} = -\frac{1}{b^2}, \quad \frac{-\frac{b}{a}}{ab} = -\frac{1}{a^2},$$

is a rational square. For example, if $\frac{1}{ab} = \square$, then $ab = \square$, and since $b = 2mn$, this implies that $ab = 4 \cdot \square$. So, we have $\frac{ab}{2} = 2 \cdot \square$, which is impossible (see [1, p. 175]). Thus, there is no pythagorean pair (k, l) such that (ak, bl) is a pythagorean pair. ■

Similar as above, we get the following

Corollary 12. *If (a, b) is a double-pythapotent pair, then there are infinitely many pythagorean pairs (k, l) , not multiples of each other, such that (ak, bl) is a pythagorean pair.*

Remark 5. Let (a, b) be a double-pythapotent pair and let (k_1, l_1) be a pythagorean pair such that (ak_1, bl_1) is a pythagorean pair. Then (k_1, l_1) is a double-pythapotent pair and we find a pythagorean pair (k_2, l_2) , which is not a multiple of (a, b) such that (k_1k_2, l_1l_2) is a pythagorean pair, which implies that (k_2, l_2) is a double-pythapotent pair. Proceeding this way, we can construct an infinite family of double-pythapotent pairs which are not multiples of each other.

Algorithm 2. The following algorithm describes how to construct pythagorean pairs (k, l) from rational points on $\Gamma_{a,b}$ of infinite order.

- Let P be a rational point on $\Gamma_{a,b}$ of infinite order and let x_2 be the x -coordinate of $2 * P$.
- Let f and g be relatively prime positive integers such that

$$\frac{g}{f} = \sqrt{x_2}.$$

- Let r and s be relatively prime positive integers such that

$$\frac{r}{s} = \frac{bf + \sqrt{g^2 + b^2f^2}}{g}.$$

- Let $k := r^2 - s^2$ and let $l := 2rs$.

Then (ak, bl) is a pythagorean pair.

Example. Let again $m = 17$, $n = 1$, $a = m^2 - n^2$, and $b = 2mn$, hence, $(a, b) = (288, 34)$. Now, the curve $\Gamma_{a,b}$, with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, has rank 2 with generators

$$P = (-81600, 2970240) \quad \text{and} \quad P' = (-58752, 9047808).$$

The x -coordinate of $2 * P$ is $\frac{5156388864}{4225}$ which leads to $(k, l) = (65, 2112)$ with

$$(288 \cdot 65)^2 + (34 \cdot 2112)^2 = 74208^2,$$

and x -coordinate of $2 * P'$ is $\frac{4161600}{121}$ which leads to $(k', l') = (11, 60)$ with

$$(288 \cdot 11)^2 + (34 \cdot 60)^2 = 3768^2.$$

Acknowledgment

We would like to thank the referee for his or her careful reading and useful comments and suggestions, which helped to improve the quality of the article.

References

- [1] Bernhard Frénicle de Bessy, *Memoires de l'Academie royale des sciences, volume tome V, La compagnie des libraires, Paris, 1729.*
- [2] Lorenz Halbeisen, Norbert Hungerbühler, A theorem of Fermat on congruent number curves, *Hardy-Ramanujan J.* 41 (2018) 15–21.
- [3] Lorenz Halbeisen, Norbert Hungerbühler, Heron triangles and their elliptic curves, *J. Number Theory* 213 (2020) 232–253.
- [4] Lorenz Halbeisen, Norbert Hungerbühler, Constructing cubic curves with involutions, arXiv:2106.08154 [org/abs], submitted for publication.
- [5] Lorenz Halbeisen, Norbert Hungerbühler, Arman Shamsi Zargar, New parametrisations of elliptic curves with torsion groups $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, and $\mathbb{Z}/14\mathbb{Z}$, arXiv:2106.06861 [org/abs], submitted for publication.
- [6] Kurt Heegner, *Diophantische Analysis und Modulfunktionen*, *Math. Z.* 56 (1952) 227–253.
- [7] Charles Henry, Paul Tannery, *Œuvres de Fermat, volume I–III*, Gauthier-Villars et Fils, Paris, 1891.
- [8] Daniel Sion Kubert, Universal bounds on the torsion of elliptic curves, *Proc. Lond. Math. Soc.* (3) 33 (2) (1976) 193–237.
- [9] F. Patrick Rabarison, Structure de torsion des courbes elliptiques sur les corps quadratiques, *Acta Arith.* 144 (1) (2010) 17–52.
- [10] Joseph H. Silverman, John Tate, *Rational Points on Elliptic Curves*, 2nd edition, Springer-Verlag, New York, 2015.
- [11] Hieronymus Georg Zeuthen, Raphael Meyer, *Geschichte der Mathematik im XVI. und XVII. Jahrhundert*, B.G. Teubner, Leipzig, 1903.