Available online at www.sciencedirect.com

ScienceDirect

Indagationes Mathematicae 36 (2025) 903–911

indagationes mathematicae

www.elsevier.com/locate/indag

Full length article

Pairing powers of pythagorean pairs

Lorenz Halbeisen[a], Norbert Hungerbühler[a,*], Arman Shamsi Zargar[b]

[a] *Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland*
[b] *Department of Mathematics and Applications, University of Mohaghegh Ardabili, Ardabil, Iran*

Received 24 May 2024; received in revised form 5 September 2024; accepted 29 September 2024

Communicated by: P. Moree

Abstract

A pair (a, b) of positive integers is a *pythagorean pair* if $a^2 + b^2$ is a square. A pythagorean pair (a, b) is called a *pythapotent pair of degree* h if there is another pythagorean pair (k, l), which is not a multiple of (a, b), such that $(a^h k, b^h l)$ is a pythagorean pair. To each pythagorean pair (a, b) we assign an elliptic curve Γ_{a^h,b^h} for $h \geq 3$ with torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ such that Γ_{a^h,b^h} has positive rank over $\mathbb{Q}$ if and only if (a, b) is a pythapotent pair of degree h. As a side result, we get that if (a, b) is a pythapotent pair of degree h, then there exist infinitely many pythagorean pairs (k, l), not multiples of each other, such that $(a^h k, b^h l)$ is a pythagorean pair. In particular, we show that any pythagorean pair is always a pythapotent pair of degree 3. In a previous work, pythapotent pairs of degrees 1 and 2 have been studied.

Keywords: Pythagorean pair, Pythapotent pair of arbitrary degree, Elliptic curve

1. Introduction

A *pythagorean pair* is a pair (a, b) of positive integers such that $a^2 + b^2$ is a square. We adopt the usual notation $a^2 + b^2 = \square$ for this. A pythagorean pair (a, b) is called a *pythapotent pair of degree* h if there is another pythagorean pair (k, l), which is not a multiple of (a, b), such that $(a^h k, b^h l)$ is also a pythagorean pair, *i.e.*,

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

* Corresponding author.
E-mail addresses: lorenz.halbeisen@math.ethz.ch (L. Halbeisen), norbert.hungerbuehler@math.ethz.ch (N. Hungerbühler), zargar@uma.ac.ir (A. Shamsi Zargar).

https://doi.org/10.1016/j.indag.2024.09.011

To simplify the language, we will call a pythapotent pair of degree 3, 4 and 5 a *cubic, quartic* and *quintic pythapotent pair*, respectively. We will also keep the definition of a double-pythapotent and quadratic pythapotent pair given in [4] that address a pythapotent pair of degree 1 and 2, respectively.

As the pair of squares (a^2, b^2) of a pythagorean pair (a, b) is never a pythagorean pair, it is natural to ask whether the Hadamard–Schur products $(a^h k, b^h \ell)$, $h \geq 1$, of pythagorean pairs can be a pythagorean pair or not. For a double-pythapotent and quadratic pythapotent pair, the question has been investigated in [4]. More precisely, it has been shown that for each pythagorean pair (a, b), the elliptic curve $\Gamma_{a,b}$ (Γ_{a^2,b^2}, resp.) has torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ($\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, resp.) and that (a, b) is a double-pythapotent (quadratic pythapotent, resp.) pair if and only if $\Gamma_{a,b}$ (Γ_{a^2,b^2}, resp.) has positive rank over $\mathbb{Q}$. With the points of infinite order on the curve $\Gamma_{a,b}$ (Γ_{a^2,b^2}, resp.) infinitely many pythagorean pairs (k, l) can be generated, not multiples of each other, such that (ak, bl) ((a^2k, b^2l), resp.) are pythagorean pairs. Moreover, 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).

In this work, we will answer affirmatively the question for $h \geq 3$, which generalizes the results of [4] concerning double-pythapotent and quadratic pythapotent pairs. The question will lead, indeed, again in a natural way to associated elliptic curves of positive rank over $\mathbb{Q}$.

For a positive integer h, we assign the elliptic curve

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

to the pythagorean pair (a, b). We will show that then the curve Γ_{a^h,b^h} with $h \geq 3$ has torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (see Proposition 2), and that (a, b) is a pythapotent pair of degree h if and only if Γ_{a^h,b^h} has positive rank over $\mathbb{Q}$ (see Theorem 3). With the points of infinite order on the curve Γ_{a^h,b^h} we can generate infinitely many pythagorean pairs (k, l), not multiples of each other, such that $(a^h k, b^h l)$ are pythagorean pairs. In particular, we show that any pythagorean pair is actually a cubic pythapotent pair (see Corollary 10).

Example. Let us have a look at an example. The pythagorean pair $(a, b) = (3, 4)$ is a quartic pythapotent pair. Indeed, for the pythagorean pair $(k, l) = (176, 57)$ we have

$$(3^4 \cdot 176)^2 + (4^4 \cdot 57)^2 = 20400^2.$$

However, since the rank of the elliptic curve $\Gamma_{3^5,4^5}$ is 0, $(3, 4)$ is not a quintic pythapotent pair. With the help of the theory of elliptic curves, we will later uncover the formulas with which such examples can be systematically generated. In particular, we will see how to find the matching pair (k, l) (see the examples in Section 2).

Remark 1. In [4], the 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, was obtained by using Schroeter's construction of cubic curves with line involutions (see [3]). 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 Γ_{a^h,b^h}, where (a, b) is a pythagorean pair, are obtained by replacing the terms $a^4 + b^4$ and a^4b^4 in the parametrization of Γ_{a^2,b^2} by $a^{2h} + b^{2h}$ and $a^{2h}b^{2h}$, respectively.

2. Pythapotent pairs of degree h

In a first step we show that for any distinct pythagorean pairs (a_1, b_1) and (a_2, b_2) with relatively prime components, *i.e.*, $\gcd(a_1, b_1) = \gcd(a_2, b_2) = 1$, and for any distinct positive integers $k \neq l$, we have

$$\frac{a_1^k - b_1^k}{a_1^k + b_1^k} \neq \frac{a_2^l - b_2^l}{a_2^l + b_2^l}.$$

With this result we then show that Γ_{a^h,b^h} has torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ for any positive integer $h \neq 2$, and it has torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ for $h = 2$. Finally, we show how we obtain pythagorean pairs (k, l) from a point on Γ_{a^h,b^h} whose x-coordinate is a square such that $(a^h k, b^h l)$ is a pythagorean pair.

Lemma 1. *If (a_1, b_1) and (a_2, b_2) are relatively prime pythagorean pairs and k and l are distinct positive integers, then*

$$\frac{a_1^k - b_1^k}{a_1^k + b_1^k} \neq \frac{a_2^l - b_2^l}{a_2^l + b_2^l}.$$

Proof. Let m_1, n_1, m_2, n_2 be positive integers such that $a_1 = m_1^2 - n_1^2$, $b_1 = 2m_1n_1$, $a_2 = m_2^2 - n_2^2$, $b_2 = 2m_2n_2$. Assume towards a contradiction that

$$\frac{a_1^k - b_1^k}{a_1^k + b_1^k} = \frac{a_2^l - b_2^l}{a_2^l + b_2^l}.$$

Then, solving this equation for the integers n_1 and n_2, respectively, we obtain that

$$a_2^{\frac{2l}{k}} + b_2^{\frac{2l}{k}} = \square \qquad \text{and} \qquad a_1^{\frac{2k}{l}} + b_1^{\frac{2k}{l}} = \square.$$

Since the components of both pairs (a_1, b_1) and (a_2, b_2) are relatively prime, we must have that $\frac{2l}{k}$ and $\frac{2k}{l}$ are integers, which implies that there are positive integers s and t such that $ks = 2l$ and $lt = 2k$. This implies that $ts = 4$, and therefore, we have either $t = 1$ and $s = 4$, $t = 4$ and $s = 1$, or $t = s = 2$. In the first case we have $l = 2k$, which gives us $a_2^4 + b_2^4 = \square$, which is impossible, in the second we obtain $a_1^4 + b_1^4 = \square$, which is also impossible, and in the third case we have $k = l$, which contradicts our assumption that k and l are distinct. □

Proposition 2. *If (a, b) is a pythagorean pair, then the elliptic curve*

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

has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ for any positive integer $h \neq 2$, and it has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ for $h = 2$.

Proof. We use Kubert's parametrization for elliptic curves with torsion group containing $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (see [6, p. 217]):

$$y^2 + xy - ey = x^3 - ex^2 \tag{1}$$

for

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

All curves in this family have a torsion group which has $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ as a subgroup, *i.e.*, by Mazur's torsion theorem, the torsion group must be either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Furthermore, it is easily seen that for $e \neq e'$, the corresponding curves in Kubert's parametrization are non-isomorphic. By replacing x by $\tilde{x} + e$ and $y + \frac{\tilde{x}}{2}$ by $\tilde{y}$ in (1) we get an elliptic curve which is isomorphic to

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

with

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

Now, for $v = \frac{p}{q}$, let $p := a^h - b^h$ and $q := 4(a^h + b^h)$. Then, if we put

$$\tilde{x} = \frac{4X}{(a^h + b^h)^2} \quad \text{and} \quad \tilde{y} = \frac{8Y}{(a^h + b^h)^3}$$

in (2), we get the equivalent curve

$$\Gamma_{a^h,b^h}: \quad Y^2 = X^3 + (a^{2h} + b^{2h})X^2 + a^{2h}b^{2h}X.$$

By Lemma 1 and the fact that the curves of the form (1) are non-isomorphic for different values of e, we get that for any pythagorean pairs (a_1, b_1) and (a_2, b_2) and for any distinct positive integers $k \neq l$, the two curves $\Gamma_{a_1^k,b_1^k}$ and $\Gamma_{a_2^l,b_2^l}$ are non-isomorphic. Notice that if (a, b) is a pythagorean pair where a and b are not relatively prime, then there is a pythagorean pair $(\bar{a}, \bar{b})$ such that the curves Γ_{a^h,b^h} and $\Gamma_{\bar{a}^h,\bar{b}^h}$ are isomorphic. This implies that for any positive integer h, the torsion group of Γ_{a^h,b^h} is either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Now we use [4, Proposition 1] which says that an elliptic curve Γ has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ if and only if there is a pythagorean pair (a, b) such that Γ is isomorphic to Γ_{a^2,b^2}. Thus, the torsion group of Γ_{a^h,b^h} is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ only when $h = 2$, and it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ otherwise. This completes the proof. □

As a matter of fact we would like to mention that the proof of Proposition 2 implies that Kubert's parametrization for elliptic curves with torsion group containing $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ gives us a curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ if and only if e is of the form

$$e = -\frac{a^2b^2}{4c^4} \quad \text{where } (a, b, c) \text{ is a pythagorean triple.}$$

Theorem 3. *The pythagorean pair (a, b) is a pythapotent pair of degree h if and only if the elliptic curve Γ_{a^h,b^h} has positive rank over $\mathbb{Q}$.*

The following Lemmatas 4, 5 and 6 prepare the proof of Theorem 3. First, we transform the curve Γ_{a^h,b^h} to another curve on which we carry out our calculations.

Lemma 4. *If $(\bar{x}, \bar{y})$, $\bar{x} \neq 0$, is a point on the curve Γ_{a^h,b^h}, then the point $(\frac{a^hb^h}{\bar{x}}, \frac{\bar{y}}{\bar{x}})$ is a point on the curve*

$$y^2x = a^hb^h + (a^{2h} + b^{2h})x + a^hb^hx^2.$$

In particular, if $(\bar{x}, \bar{y})$ is a rational point, then so is $(\frac{a^hb^h}{\bar{x}}, \frac{\bar{y}}{\bar{x}})$.

Proof. If $(\bar{x}, \bar{y})$ lies on Γ_{a^h,b^h}, then $(\bar{X}, \bar{Y}, \bar{Z}) = (a^hb^h, \bar{y}, \bar{x})$ is a point on the projective curve

$$XY^2 = a^hb^hZ^3 + (a^{2h} + b^{2h})XZ^2 + a^hb^hX^2Z.$$

Since $\bar{x} = \bar{Z} \neq 0$, the point $(\bar{X}, \bar{Y}, \bar{Z})$ also satisfies the dehomogenized equation

$$\frac{X}{Z}\Big(\frac{Y}{Z}\Big)^2 = a^h b^h + (a^{2h} + b^{2h})\frac{X}{Z} + a^h b^h \Big(\frac{X}{Z}\Big)^2.$$

Hence, $(\frac{\bar{X}}{\bar{Z}}, \frac{\bar{Y}}{\bar{Z}}) = (\frac{a^h b^h}{\bar{x}}, \frac{\bar{y}}{\bar{x}})$ is a point on the affine curve

$$y^2 x \;=\; a^h b^h + (a^{2h} + b^{2h})x + a^h b^h x^2,$$

as claimed. □

We will now use the group structure on elliptic curves to add points. In particular we will write $[2]P$ to denote the point $P + P$.

Lemma 5. *Let $P = (x_1, y_1)$ be a rational point on Γ_{a^h,b^h} and let x_2 be the x-coordinate of the point $[2]P$. Then, $x_0 := \frac{a^h b^h}{x_2}$—which is the x-coordinate of the point on the curve $y^2 x = a^h b^h + (a^{2h} + b^{2h})x + a^h b^h x^2$ which corresponds to $[2]P$— can be written as $x_0 = \frac{p}{q}$, where $q = \tilde{q}^2$ and $p = a^h b^h \cdot \tilde{p}^2$ for some $\tilde{q}, \tilde{p} \in \mathbb{Q}$, and where p and q satisfy*

$$a^h \cdot (a^h q + b^h p) \;=\; \square \qquad \text{and} \qquad b^h \cdot (a^h p + b^h q) \;=\; \square. \tag{3}$$

Proof. By Silverman and Tate [7, p. 27] we have

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

and therefore we obtain

$$x_0 \;=\; \frac{a^h b^h}{x_2} \;=\; \frac{4y_1^2\, a^h b^h}{(x_1^2 - B)^2}.$$

Thus we have $x_0 = \frac{p}{q}$ for $q = \tilde{q}^2$ and $p = a^h b^h \cdot \tilde{p}^2$ with $\tilde{p} = 2y_1$ and $\tilde{q} = x_1^2 - B$.

Now, for

$$p = 4\, a^h b^h (x_1^3 + (a^{2h} + b^{2h})x_1^2 + a^{2h} b^{2h} x_1) \quad \text{and} \quad q = (x_1^2 - a^{2h} b^{2h})^2,$$

we obtain

$$a^h \cdot (a^h q + b^h p) \;=\; a^{2h}\big(a^{2h} b^{2h} + 2b^{2h} x_1 + x_1^2\big)^2 \;=\; \square$$

and

$$b^h \cdot (a^h p + b^h q) \;=\; b^{2h}\big(a^{2h} b^{2h} + 2a^{2h} x_1 + x_1^2\big)^2 \;=\; \square$$

which completes the proof. □

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

Lemma 6. *Let (a, b) be a pythagorean pair. Then every pythagorean pair (k, l) such that $(a^h k, b^h l)$ is a pythagorean pair corresponds to a rational point on Γ_{a^h,b^h} whose x-coordinate is a square, and vice versa.*

Proof. Let $x_2 = g^2/f^2$ be the x-coordinate of a rational point $[2]P$ on Γ_{a^h,b^h} for some rational values f and g. Then, by Lemma 5, $\frac{a^h b^h}{x_2} = \frac{a^h b^h \cdot f^2}{g^2}$, where $p = a^h b^h \cdot f^2$ and $q = g^2$ satisfy (3),

i.e., $a^{2h}g^2 + a^{2h}b^{2h}f^2 = \square$, and $b^{2h}g^2 + a^{2h}b^{2h}f^2 = \square$. So,

$$\left(\frac{g}{f}\right)^2 + b^{2h} = \rho^2 \text{ for some } \rho \in \mathbb{Q}, \tag{4}$$

and $\left(\frac{g}{f}\right)^2 + a^{2h} = \square$. Let $\frac{g}{f} = \frac{2\rho t}{t^2+1}$ and $b^h = \frac{\rho(t^2-1)}{t^2+1}$. Then $\rho = \frac{b^h(t^2+1)}{t^2-1}$ and $\frac{g}{f} = \frac{2b^h t}{t^2-1}$, which gives us

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

It follows from (4) that t is a rational number, say $t = \frac{r}{s}$. Finally, since $\left(\frac{g}{f}\right)^2 + a^{2h} = \square$, we obtain

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

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

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

which shows that (a, b) is a pythapotent pair of degree h.

Assume now that we find a pythagorean pair (k, l) such that $(a^h k, b^h l)$ 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 r, s, a, b we can compute $x_2 = \frac{b^{2h}l^2}{k^2}$, which is the x-coordinate of a rational point on Γ_{a^h,b^h} whose x-coordinate is obviously a square. □

We are now ready for the proof of the main theorem.

Proof of Theorem 3. 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 6 it is enough to show that no rational point with square x-coordinate has finite order. Notice that if P is a point of infinite order, then for every integer i, $[2i]P$ is a rational point on Γ_{a^h,b^h} 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^h,b^h} with $h \geq 3$. For simplicity, we consider the 8 torsion points on the equivalent curve

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

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 $(-\frac{a^h}{b^h}, 0)$ and $(-\frac{b^h}{a^h}, 0)$, and the four points of order 4, which correspond to the four points on the curve where the tangent to the curve is parallel to the x-axis, are $\big(1, \pm(a^h + b^h)\big)$ and $\big(-1, \pm(a^h - b^h)\big)$. The corresponding points on the curve Γ_{a^h,b^h} are the three points $(0, 0)$, $(-b^{2h}, 0)$ and $(-a^{2h}, 0)$ of order 2, and the four points $\big(a^h b^h, \pm a^h b^h(a^h + b^h)\big)$ and $\big(-a^h b^h, \pm a^h b^h(a^h - b^h)\big)$ of order 4. Since x_2 is a square, we have that none of the values

$$0, \qquad -a^{2h}, \qquad -b^{2h}, \qquad a^h b^h, \qquad -a^h b^h,$$

is a rational square, except 0 and possibly $a^h b^h$. If $x_2 = 0$, then this implies $l = 0$, but $(k, 0)$ is not a pythagorean pair. If h is odd, $a^h b^h$ cannot be a square unless $ab = \square$, but it is impossible because it is equivalent to the rank 0 congruent number elliptic curve $y^2 = x^3 - x$

(also see [2, p. 175]). Consider now the case when h is even. For the case $h = 2$ see [4]. For $h \geq 4$, recall that $x_2 = \frac{b^{2h}l^2}{k^2}$ where k and l are relatively prime. Now, if $x_2 = a^h b^h$, then $l^2 = a^h b^{-h} k^2$, and therefore $(a^h k)^2 + (b^h l)^2 = a^h k^2 (a^h + b^h)$. Thus, if $(a^h k)^2 + (b^h l)^2 = \square$, then also $a^h(a^h + b^h) = \square$, and since h is even, also

$$a^h + b^h = \square.$$

However, since $h \geq 4$, by [1, Main Theorem 2] this is impossible. Thus, there is no pythagorean pair (k, l) such that $(a^h k, b^h l)$ is a pythagorean pair. $\square$

Corollary 7. *If (a, b) is a pythapotent pair of degree h, then there are infinitely many pythagorean pairs (k, l), not multiples of each other, such that $(a^h k, b^h l)$ is a pythagorean pair.*

Proof. By Theorem 3, there exists a point P on Γ_{a^h, b^h} of infinite order. Now, for every integer i, $[2i]P$ is a rational point on Γ_{a^h, b^h} 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 pairs. Thus, there are infinitely many integers j, such that the pythagorean pairs $(k_{[2j]P}, l_{[2j]P})$ are not multiples of each other. $\square$

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

- Let P be a rational point on Γ_{a^h, b^h} 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
$$\frac{r}{s} = \frac{b^h f + \sqrt{g^2 + b^{2h} f^2}}{g}.$$
- Let $k := r^2 - s^2$ and let $l := 2rs$.

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

Examples. For $m = 2$ and $n = 1$, let $a = m^2 - n^2$ and $b = 2mn$. Then $(a, b) = (3, 4)$ is a pythagorean pair and we have:

1. For $h = 1, 2, 5, 7, 10$, the rank of Γ_{a^h, b^h} is 0. Hence, $(3, 4)$ is not a pythapotent pair of degree h for these h's.
2. The curve Γ_{a^3, b^3}, with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, has rank 1 with generator $P = (-3888, 50544)$. The x-coordinate of $[2]P$ is 120^2 which leads to $(k, l) = (8, 15)$ with
$$(3^3 \cdot 8)^2 + (4^3 \cdot 15)^2 = 984^2.$$
In particular, $(3, 4)$ is a cubic pythapotent pair.

3. The curve Γ_{a^4,b^4}, with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, has rank 1 with generator $P = (-11616, 1779360)$. The x-coordinate of $[2]P$ is $\left(\frac{912}{11}\right)^2$ which leads to $(k, l) = (176, 57)$ with
$$(3^4 \cdot 176)^2 + (4^4 \cdot 57)^2 = 20400^2.$$
In particular, $(3, 4)$ is a quartic pythapotent pair.
4. The curve Γ_{a^6,b^6}, with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, has rank 1 with generator $P = \left(\frac{46022656}{9}, -\frac{678725632000}{27}\right)$. The x-coordinate of $[2]P$ is $\left(\frac{3542528}{10335}\right)^2$ which leads to $(k, l) = (82680, 6919)$ with
$$(3^6 \cdot 82680)^2 + (4^6 \cdot 6919)^2 = 66603976^2.$$
In particular, $(3, 4)$ is a pythapotent pair of degree 6.

We now have a closer look at the degrees $h = 1, 2, 3$. Corollaries 8 and 9 specify concrete conditions which imply that a pythagorean pair (a, b) is a pythapotent pair of degree 1 and 2 respectively, while Corollary 10 shows that a pythagorean pair (a, b) is automatically a cubic pythapotent pair.

Corollary 8. *Let (a, b) be a pythagorean pair with $a = m^2 - n^2$ and $b = 2mn$ such that at least one of the following two conditions is satisfied:*

$$(i)\ 5m^2 - n^2 = \square \qquad (ii)\ m^2 + 3mn + n^2 = \square$$

Then (a, b) is a double-pythapotent pair.

Notice that both conditions in Corollary 8 are satisfied for infinitely many pairs (m, n) leading to pythagorean pairs (a, b).

Proof. One gets the quadratic conditions in the statement by imposing each of the points with x-coordinates $n^2(m^2 - n^2)$ and $mn(m - n)^2$ on the curve $\Gamma_{a,b}$ respectively. In the first case, the right hand side of the equation $y^2 = x(x + a^2)(x + b^2)$ becomes $n^4(5m^2 - n^2)(m^3 - mn^2)^2$, and in the second case we get $m^2n^2(m - n)^4(m + n)^2(m^2 + 3\,mn + n^2)$. The result is then obtained from [4, Algorithm 1]. □

Corollary 9. *Let (a, b) be a pythagorean pair with $a = m^2 - n^2$ and $b = 2mn$ such that at least one of the following conditions (i)–(iii) is satisfied.*

$$(i)\ -m^4 - 4mn^3 + n^4 = \square$$
$$(ii)\ m^4 + 4m^2n^2 - n^4 = \square$$
$$(iii)\ m^4 - 2m^3n + 2m^2n^2 + 2mn^3 + n^4 = \square$$

Then (a, b) is a quadratic pythapotent pair.

Proof. The quartic conditions (i)–(iii) are obtained by imposing each of the points with x-coordinates $-8m^2n^4(m+n)^2$, $8m^4n^2(m^2-n^2)$, $8m^3n^3(m^2-n^2)$, on the curve Γ_{a^2,b^2} respectively. Note that each of the quartic conditions (i)–(iii) is equivalent to an elliptic curve of rank one. The result then follows from [4, Algorithm 2]. □

Corollary 10. *Let (a, b) be a pythagorean pair. Then (a, b) is a cubic pythapotent pair.*

Proof. Let $a = m^2 - n^2$ and $b = 2mn$. Since the curve Γ_{a^3,b^3} owns the non-obvious rational point

$$P = \big(-16(m^2-n^2)^2m^4n^4,\, 16(m^2-n^2)^2m^4n^4(m^2+n^2)(m^4-6m^2n^2+n^4)\big),$$

the result immediately comes from our Algorithm above as follows. The x-coordinate of the point $[2]P$ is

$$\big(2m^2n^2(m-n)^2(n+m)^2/(m^2+n^2)\big)^2$$

which, by applying our Algorithm, leads to

$$k = 4mn(m^2+n^2), \qquad l = (m-n)^2(n+m)^2,$$

with

$$(a^3k)^2 + (b^3l)^2 = (4mn(m^4+n^4)(m-n)^2(n+m)^2)^2. \quad \square$$

We conclude the paper with two open problems.

Question 1. *Take an arbitrary pythagorean pair (a, b). Is there an $h \geq 4$ such that (a, b) is a pythapotent pair of degree h?*

Question 2. *Take an arbitrary $h \geq 4$. Is there a pythagorean pair (a, b) which is a pythapotent pair of degree h? Or equivalently: Is there a pythagorean pair (a, b) such that Γ_{a^h,b^h} has positive rank over $\mathbb{Q}$?*

Notice that Corollary 10 answers both questions for $h = 3$. Corollaries 8 and 9 give partial answers to Question 1 for $h = 1$ and $h = 2$ respectively.

Acknowledgement

We are grateful to the referees for the valuable comments that helped improve this article. The third author would like to thank ETH Zürich for its hospitality.

References

[1] Henri Darmon, Loïc Merel, Winding quotients and some variants of fermat's last theorem, J. Reine Angew. Math. [Crelle's J.] 490 (1997) 81–100.
[2] Bernhard Frénicle de Bessy, Memoires de l'Academie Royale Des Sciences, vol. tome V, La compagnie des libraires, Paris, 1729.
[3] Lorenz Halbeisen, Norbert Hungerbühler, Constructing cubic curves with involutions, Beiträge Algebra Geom. / Contrib. Algebra Geom. 63 (2022) 921–940.
[4] Lorenz Halbeisen, Norbert Hungerbühler, Pairing pythagorean pairs, J. Number Theory 233 (2022) 467–480.
[5] Lorenz Halbeisen, Norbert Hungerbühler, Arman Shamsi Zargar, Maksym Voznyy, A geometric approach to elliptic curves with torsion groups $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, and $\mathbb{Z}/16\mathbb{Z}$, Rad. Hrvat. Akad. Znan. Umjetnosti. Mat. Znan. 27 (2023) 87–109.
[6] Daniel Sion Kubert, Universal bounds on the torsion of elliptic curves, Proc. Lond. Math. Soc. (3) 33 (2) (1976) 193–237.
[7] Joseph H. Silverman, John Tate, Rational Points on Elliptic Curves, 2nd ed., Springer-Verlag, New York, 2015.