Math Semesterber (2020) 67:213–236
https://doi.org/10.1007/s00591-020-00279-z

MATHEMATIK IN FORSCHUNG UND ANWENDUNG

# Four rational squares in arithmetic progressions and a family of elliptic curves with positive Mordell-Weil rank

**Hagen Knaf · Erich Selder · Karlheinz Spindler**

Received: 27 August 2019 / Accepted: 10 April 2020 / Published online: 30 June 2020


**Abstract** We study the question at which relative distances four squares of rational numbers can occur as terms in an arithmetic progression. This number-theoretical problem is seen to be equivalent to finding rational points on certain elliptic curves. Both number-theoretical results and results concerning the associated elliptic curves are derived; i.e., the correspondence between rational squares in arithmetic progressions and elliptic curves is exploited both ways.

**Keywords** Number theory · Elliptic curves

**Mathematics Subject Classification** 11 D 09 · 11 G 05 · 14 E 05

## 1 Introduction

In 1640, Fermat found that there are no four equidistantly spaced squares of rational numbers. One can ask a more general question: Given a triplet $(k, \ell, m)$ of natural numbers, are there rational numbers $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$ and a step size $s > 0$ such that $\beta^2 - \alpha^2 = ks$, $\gamma^2 - \beta^2 = \ell s$ and $\delta^2 - \gamma^2 = ms$? It turns out that this question is equivalent to finding rational points on the elliptic curve $E_{k,\ell,m}$ given by the

H. Knaf · K. Spindler (✉)
Hochschule RheinMain, Wiesbaden, Germany
E-Mail: Karlheinz.Spindler@hs-rm.de

H. Knaf
E-Mail: Hagen.Knaf@hs-rm.de

E. Selder
Frankfurt University of Applied Sciences, Frankfurt, Germany
E-Mail: e_selder@fb2.fra-uas.de

affine equation $y^2 = x(x + km)(x + (k + \ell)(\ell + m))$. Consequently, one can use the theory of elliptic curves to draw various conclusions on the original number-theoretical problem.

Remarkably, this approach also works the other way: Rather trivial number-theoretical facts can be used to derive nontrivial results on the associated elliptic curves. Specifically, a rather large class of elliptic curves is shown to have positive rank, and this is done in an elementary way which, in addition, gives an explicit construction of an element of infinite order on the elliptic curve in question. As the problem discussed here is strongly linked with other number-theoretical problems such as the concordant form problem and the problem of $\theta$-congruent numbers, we start out by providing some historical context and perspective for the topic at hand.

## 2 Historical overview

### 2.1 The congruent number problem

A number $n \in \mathbb{N}$ is called *congruent* if there are rational numbers $\alpha, \beta, \gamma \in \mathbb{Q}$ such that $\alpha^2 < \beta^2 < \gamma^2$ is an arithmetic progression with step size $n$, i.e., if $\gamma^2 - \beta^2 = \beta^2 - \alpha^2 = n$. (In other words, $n$ is congruent if and only if there is a rational square $\xi^2$ such that $\xi^2 \pm n$ are also rational squares.) The problem is then to decide whether or not a given number $n \in \mathbb{N}$ is congruent. This problem, which can be traced back to an Arab manuscript written before 972 (see [7], Chapter XVI, p. 459), is more than a thousand years old. It was solved in 1983 by Tunnell (see [44]) modulo a weak version of the Birch-Swinnerton-Dyer conjecture.

Before giving some examples, we note that the congruent number problem can be clothed in geometric language. Namely, a number $n$ is congruent if and only if there is a right triangle with rational sides $a, b, c$ which has $n$ as its area. To wit: If $0 \leq \alpha < \beta < \gamma$ are rational numbers such that

$$\beta^2 - \alpha^2 = n \quad \text{and} \quad \gamma^2 - \beta^2 = n, \tag{1}$$

then the rational numbers $a := \gamma - \alpha$, $b := \gamma + \alpha$ and $c := 2\beta$ satisfy the conditions

$$0 < a \leq b < c, \quad a^2 + b^2 = c^2 \quad \text{and} \quad n = ab/2 \tag{2}$$

and hence yield a triangle with the properties mentioned. Conversely, given such a triangle and hence given rational numbers $a, b, c$ satisfying (2), then the numbers $\alpha := (b - a)/2$, $\beta := c/2$ and $\gamma := (b + a)/2$ provide a solution of (1). Now let us look at some examples, noticing by the way that a number $n$ is congruent if and only if its square-free part is congruent, so that it is enough to consider square-free numbers.

The number 6 is congruent, as can be seen from the progression $(1/2)^2 < (5/2)^2 < (7/2)^2$ or from the triangle with sides $a = 3$, $b = 4$ and $c = 5$. The

number 5 is congruent, as can be seen from the progression $(31/12)^2 < (41/12)^2 < (49/12)^2$ or from the triangle with sides $a = 3/2$, $b = 20/3$ and $c = 41/6$. This last example has some historical interest; it dates back to Leonardo of Pisa, known as Fibonacci, to whom the problem was presented by John of Palermo at the court of Frederick II around 1220. The problem and its solution are mentioned in Leonardo's memoir *Flos*; the derivation of the solution is explained in the *Liber quadratorum*. (See [4], pp. 1430/1431.) The number 2 is not congruent, as can be derived from the fact that the equation $u^4 + v^4 = w^2$ has no solution in natural numbers (a fact which, in turn, can be deduced from the theory of Pythagorean triplets). More on the older history of the congruent number problem can be found in [7], chapter XVI. In a well-known article (see [51]), Zagier showed that 157 is a congruent number by establishing the fact that the triangle with sides

$$\begin{aligned} a &= \frac{411340519227716149383203}{21666555693714761309610}, \\ b &= \frac{6803298487826435051217540}{411340519227716149383203}, \\ c &= \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830} \end{aligned} \tag{3}$$

is a right triangle whose area is 157. It is clear that one does not find such solutions by trial and error. In fact, gaining any deeper insights into the congruent number problem involves a connection to the theory of elliptic curves, which will be explained later.

### 2.2 Variants of the congruent number problem

The congruent number problem in its geometric formulation can be easily generalized by asking which natural numbers $n$ can occur as the area of an arbitrary (not necessarily right) triangle with rational sides. Denoting the sides of such a triangle by $a, b, c$ and the angle opposite $c$ by $\theta$, this amounts to finding rational numbers $a, b, c$ and a number $0 < \theta < \pi$ such that $c^2 = a^2 + b^2 - 2ab\cos(\theta)$ and $n = ab\sin(\theta)/2$. Then $(\cos(\theta), \sin(\theta))$ is automatically a rational point on the unit circle other than $(\pm 1, 0)$ and hence must have the form $((t^2-1)/(t^2+1), 2t/(1+t^2))$ with a rational number $t > 0$. Thus an integer $n$ is called $t$-congruent for a given rational number $t > 0$ if there are rational numbers $a, b, c > 0$ such that

$$c^2 = a^2 + b^2 - 2ab \cdot \frac{t^2-1}{t^2+1} \quad \text{and} \quad n = \frac{abt}{1+t^2}. \tag{4}$$

(Clearly, a number $n$ is 1-congruent if and only if it is congruent in the sense defined before. The concept of $t$-congruence, albeit without using the name, is introduced in [25], pp. 8/9, Problem 3.) More generally, if a triangle has rational sides $a, b, c$ and if $\theta$ is the angle opposite $c$ then $\cos(\theta)$ is necessarily rational, say $\cos(\theta) = r/s$ in reduced form, and the area of this triangle is given by $F = ab\sin(\theta)/2 = ab\sqrt{s^2 - r^2}/(2s)$. Given a number $n \in \mathbb{N}$ we can then ask whether or

not there is such a triangle with $F = n\sqrt{s^2 - r^2}$. Thus given an angle $\theta \in (0, \pi)$ for which $\cos(\theta) = r/s$ is rational, a natural number $n$ is called $\theta$-congruent if there is a triangle with rational sides which has $\theta$ as an angle and $n\sqrt{s^2 - r^2}$ as its area, i.e., if there are rational numbers $a, b, c > 0$ such that $c^2 = a^2 + b^2 - 2abr/s$ and $n = ab/(2s)$. The problem is then to decide whether or not a given number $n \in \mathbb{N}$ is $\theta$-congruent for some suitable angle $\theta$; see [10, 11, 17, 22, 43, 48–50] and also [5] and [27] for related work. Clearly, a $(\pi/2)$-congruent number is the same as a congruent number in the above sense. The only other angles $\theta$ for which $\theta$-congruence has been studied somewhat systematically are $\theta = \pi/3$ and $\theta = 2\pi/3$; see [29, 43] and [20] as references.

### 2.3 Euler's concordant form problem

Let $m, n \in \mathbb{Z} \setminus \{0\}$ be integers with $m \neq n$. Following Euler (see [8]), the quadratic forms $X^2 + mY^2$ and $X^2 + nY^2$ (or the numbers $m$ and $n$ themselves) are called *concordant* if there are integers $(X, Y, Z, W)$ with $Y \neq 0$ such that

$$X^2 + mY^2 = Z^2, \qquad X^2 + nY^2 = W^2. \tag{5}$$

On the other hand, if this system of quadratic equations admits only the trivial solutions $(X, 0, \pm X, \pm X)$ then the quadratic forms $X^2 + mY^2$ and $X^2 + nY^2$ (or the numbers $m$ and $n$ themselves) are called *discordant*. The concordant form problem is then to decide whether or not two given nonzero integers $m \neq n$ are concordant; cf. [2, 7, 32, 33]. Letting $\alpha := X/Y$ in the above equations, this amounts to asking whether or not there is a rational square $\alpha^2$ such that $\alpha^2 + m$ and $\alpha^2 + n$ are also rational squares. Clearly, a number $n$ is congruent if and only if $n$ and $-n$ are concordant; hence Euler's problem generalizes the congruent number problem. One can readily check (see [37]) that there is a 1-1 correspondence between the solutions of the $\theta$-congruent number problem and Euler's concordant form problem, but since the geometric formulation of the problem is somewhat contrived we do not go into any details in this direction, but rather point out how Euler's problem gives rise to a more general problem in a rather natural way.

### 2.4 Squares in arithmetic progression

The congruent number problem amounts to identifying all triplets of rational squares in arithmetic succession. Euler's concordant form problem amounts to identifying all triplets of rational squares which occur in an arithmetic progression, but not necessarily in immediate succession. The same questions can be asked for four rather than three squares. The first question has a negative answer: As was already known to Fermat (who formulated the fact in a letter to Frenicle in 1640 without proving it), there are no rational numbers $\alpha, \beta, \gamma, \delta$ such that $\beta^2 - \alpha^2 = \gamma^2 - \beta^2 = \delta^2 - \gamma^2$. (A proof of this fact can be given by using the method of infinite descent; see for example [18], pp. 112/113. Note that Fermat's old problem still gave rise to priority disputes at the beginning of the 21st century; cf. [1, 6] and [45].) On the other hand, the analogue of Euler's problem for four squares turns out to be

a meaningful and rather interesting problem: Given a triplet $(k, \ell, m)$ of natural numbers, decide whether or not there is a rational square $\alpha^2$ for which $\alpha^2 + k$, $\alpha^2 + \ell$ and $\alpha^2 + m$ are also rational squares. (Clearing denominators, this means that we are looking for four integer squares which are separated by the $k$-fold, the $\ell$-fold and the $m$-fold of a common step size.) Note that this generalization of Euler's problem has overlaps with the problem of identifying arithmetic progressions of squares in quadratic number fields such as $7^2 < 13^2 < 17^2 < (\sqrt{409})^2 < 23^2$ in $\mathbb{Q}(\sqrt{409})$, which has recently been investigated (cf. [13, 14, 47]). See also [3, 15] and [35] for generalizations in a different direction.

### 2.5 The role of elliptic curves

It is difficult to say who first made the connection between the number-theoretical problems described above and the theory of elliptic curves, but inklings of such a connection date back to Euler 1780 (see [8]), Jacobi 1835 (see [19]), Kummer 1848 (see [26]) and Lucas 1877 (see [30]). However, the fundamental role of elliptic curves could not have become clear before the discovery of the group structure on such a curve, which seems to be due to Juel in 1896 (see [21]), and the first mathematician who exploited the theory of elliptic curves in a nontrivial way to make progress on the congruent number problem seems to be Heegner in 1952 (see [16]), who proved, amongst other things, that if $p$ is a prime such that $p \equiv 5$ or $p \equiv 7$ modulo 8 then $p$ is congruent. The first explicit mentioning of the fundamental role of elliptic curves to approach the congruent number problem we are aware of dates from as late as 1975 (see [28]), and since then all substantial progress which has been made towards solving the congruent number problem and the concordant form problem rests on reformulating these problems as problems of finding rational points on certain elliptic curves; cf. [34, 39, 41, 42, 44]. The textbook [25] actually bases an introduction to elliptic curves and modular forms on the congruent number problem. It is therefore instructive to see how the connection is made in this textbook.

Given a right triangle with rational sides $a, b, c$ (where $c$ is the hypotenuse) and area $n = ab/2$, we can form the numbers $x := c^2/4$ and $y := (a^2 - b^2)c/8$, which are obviously rational and satisfy the equation

$$\begin{aligned} x(x-n)(x+n) = x(x^2-n^2) &= \frac{c^2}{4}\left(\frac{c^4}{16} - \frac{a^2b^2}{4}\right) = \frac{c^2(c^4 - 4a^2b^2)}{64} \\ &= \frac{c^2((a^2+b^2)^2 - 4a^2b^2)}{64} = \frac{c^2(a^2-b^2)^2}{64} = y^2, \end{aligned} \tag{6}$$

which shows that $(x, y)$ is a rational point on the elliptic curve given by the equation $y^2 = x(x-n)(x+n)$. Thus the approach taken in [25] consists in using the mapping $(a, b, c) \mapsto (c^2/4, (a^2-b^2)c/8)$ to assign to each (rational) point in the solution set of the equations $a^2 + b^2 = c^2$ and $n = ab/2$ (which, geometrically speaking, is the intersection of a double cone with a hyperbolic cylinder in three-space) a (rational) point on the elliptic curve given by the equation $y^2 = x(x-n)(x+n)$. Similarly, in [32], the problem of finding nontrivial solutions of the equations $X^2+mY^2 = Z^2$ and $X^2 + nY^2 = W^2$ is transformed to the problem of finding rational points on some elliptic curve as follows: Letting $x := X^2/Y^2$, the two equations become $x + m = Z^2/Y^2$ and $x + n = W^2/Y^2$; hence letting $y := XZW/Y^3$ we have

$$x(x+m)(x+n) = \frac{X^2}{Y^2} \cdot \frac{Z^2}{Y^2} \cdot \frac{W^2}{Y^2} = \left(\frac{XZW}{Y^3}\right)^2 = y^2, \tag{7}$$

which shows that $(x, y)$ is a rational point on the elliptic curve given by the equation $y^2 = x(x+m)(x+n)$. As was pointed out (and remedied) in [37], in both cases the mappings chosen are not isomorphisms between algebraic varieties, but only mappings of degree 4, which causes a loss of information on effects corresponding to torsion points on the elliptic curve in question. In [23], we gave an explicit (and lavishly illustrated) general construction of a rationally defined isomorphism between a rationally defined smooth intersection of two quadrics in projective three-space and an elliptic curve in Weierstraß form which maps a distinguished rational point in the intersection of the two quadrics to the point at infinity of the elliptic curve. This construction works not only for the congruent number problem and the concordant form problem, but also for the problem of four squares in an arithmetic progression, which we are going to study now.

## 3 Rational squares in arithmetic progressions and elliptic curves

We now turn to the question of finding four rational squares which form part of an arithmetic progression. To have a succinct terminology available, let us give the following definition.

**Definition 1** Given natural numbers $k$, $\ell$, $m \in \mathbb{N}$, we say that four squares $\alpha^2 \le \beta^2 \le \gamma^2 \le \delta^2$ of rational numbers $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$ form a **progression of type** $(\boldsymbol{k}, \boldsymbol{\ell}, \boldsymbol{m})$ if there is a number $s \ge 0$ (necessarily rational) such that

$$\beta^2 - \alpha^2 = ks, \quad \gamma^2 - \beta^2 = \ell s, \quad \delta^2 - \gamma^2 = ms. \tag{8}$$

Such a progression is called **trivial** if $s = 0$.

We note that if $\beta^2 - \alpha^2 = ks$, $\gamma^2 - \beta^2 = \ell s$ and $\delta^2 - \gamma^2 = ms$ with a negative step size $s < 0$ then the squares $\delta^2 < \gamma^2 < \beta^2 < \alpha^2$ form a progression of type $(m, \ell, k)$ with the positive step size $-s$. If (8) holds for a fixed triplet $(k, \ell, m)$, then

$\ell(\beta^2-\alpha^2) = \ell ks = k\ell s = k(\gamma^2-\beta^2)$ and $m(\gamma^2-\beta^2) = m\ell s = \ell ms = \ell(\delta^2-\gamma^2)$ so that

$$(k+\ell)\beta^2 - k\gamma^2 - \ell\alpha^2 = 0 \quad \text{and} \quad -m\beta^2 + (m+\ell)\gamma^2 - \ell\delta^2 = 0. \tag{9}$$

Conversely, if $\alpha, \beta, \gamma, \delta$ are such that (9) holds for a given triplet $(k, \ell, m) \in \mathbb{N}^3$, we can define

$$s := \frac{\beta^2-\alpha^2}{k} = \frac{\gamma^2-\beta^2}{\ell} = \frac{\delta^2-\gamma^2}{m} \tag{10}$$

to get a solution of the original problem (8). Thus given a triplet $(k, \ell, m)$, we ask whether or not the system (9) admits a nontrivial solution $(\alpha, \beta, \gamma, \delta) \neq \lambda \cdot (\pm 1, \pm 1, \pm 1, \pm 1)$ in rational numbers. Since the equations in (9) are homogeneous, we can interpret $\alpha, \beta, \gamma, \delta$ as projective coordinates of a point in $\mathbb{P}^3(\mathbb{Q})$, and condition (9) can be reformulated by stating that the point $(X_0, X_1, X_2, X_3) := (\beta, \gamma, \alpha, \delta) \in \mathbb{P}^3(\mathbb{C})$ is a rational point in the intersection of the two quadrics given by the equations $(k+\ell)X_0^2 - kX_1^2 - \ell X_2^2 = 0$ and $-mX_0^2 + (m+\ell)X_1^2 - \ell X_3^2 = 0$. This is a key observation for the approach to be presented in this paper and gives rise to the following definition.

**Definition 2** Given natural numbers $k$, $\ell$, $m \in \mathbb{N}$, we let

$$Q_{k,\ell,m} := Q^{(1)}_{k,\ell,m} \cap Q^{(2)}_{k,\ell,m} \tag{11}$$

where

$$\begin{aligned} Q^{(1)}_{k,\ell,m} &:= \left\{(X_0, X_1, X_2, X_3) \in \mathbb{P}^3(\mathbb{C}) \mid (k+\ell)X_0^2 = kX_1^2 + \ell X_2^2\right\}, \\ Q^{(2)}_{k,\ell,m} &:= \left\{(X_0, X_1, X_2, X_3) \in \mathbb{P}^3(\mathbb{C}) \mid (m+\ell)X_1^2 = mX_0^2 + \ell X_3^2\right\}. \end{aligned} \tag{12}$$

We note that $Q_{k,\ell,m}$ always (independently of the values of $k$, $\ell$ and $m$) contains the eight trivial rational points $(1, \pm 1, \pm 1, \pm 1)$, each of which represents a trivial progression; hence the task at hand is to find nontrivial rational points on $Q_{k,\ell,m}$. Now it will turn out (see Theorem 1 below) that there is a rationally defined isomorphism which maps $Q_{k,\ell,m}$ to the elliptic curve with the affine equation $y^2 = x(x+km)(x+(k+\ell)(\ell+m))$, for which we also introduce some notation.

**Definition 3** Given natural numbers $k$, $\ell$, $m \in \mathbb{N}$, we let

$$E_{k,\ell,m} := \left\{(X, Y, T) \in \mathbb{P}^2(\mathbb{C}) \mid Y^2T = X(X+kmT)(X+(k+\ell)(\ell+m)T)\right\} \tag{13}$$

and denote by $T_{k,\ell,m}$ the torsion group of the Mordell-Weil group of $E_{k,\ell,m}$, which consists of all rational points on $E_{k,\ell,m}$. The rank of this Mordell-Weil group will be simply called the rank of $E_{k,\ell,m}$.

The Mordell-Weil group of $E_{k,\ell,m}$ obviously possesses three points of order 2, namely $(0,0,1)$, $(-km,0,1)$ and $(-(k+\ell)(\ell+m),0,1)$, and hence contains $\mathbb{Z}_2\times\mathbb{Z}_2$ in its torsion group. In [23], the following result was derived. (Cf. also Appendix A.3 in [12].)

**Theorem 1** There is an isomorphism $\Phi : Q_{k,\ell,m} \to E_{k,\ell,m}$ which maps the eight trivial points $(1,\pm1,\pm1,\pm1)$ to rational points on the elliptic curve $E_{k,\ell,m}$ as follows:

$$\begin{aligned}
P_0 &:= \Phi(1,\ 1,\ 1,\ 1) = (0,1,0),\\
P_1 &:= \Phi(1,\ 1,-1,-1) = (0,0,1),\\
P_2 &:= \Phi(1,-1,\ 1,-1) = (-(k+\ell)(\ell+m),\ 0,\ 1),\\
P_3 &:= \Phi(1,-1,-1,1) = (-km,0,1),\\
P_4 &:= \Phi(1,\ 1,\ 1,-1) = (m(\ell+m),\ m(\ell+m)(k+\ell+m),\ 1),\\
P_5 &:= \Phi(1,\ 1,-1,1) = (k(k+\ell),\ -k(k+\ell)(k+\ell+m),\ 1),\\
P_6 &:= \Phi(1,-1,\ 1,\ 1) = (-m(k+\ell),\ -m\ell(k+\ell),\ 1),\\
P_7 &:= \Phi(1,-1,-1,-1) = (-k(\ell+m),\ k\ell(\ell+m),\ 1).
\end{aligned} \tag{14}$$

Note that $P_0$ is the point at infinity and $P_1, P_2, P_3$ are the points of order 2. The numbering of the points is chosen such that $P_{i+4} = P_i + P_4$ for $i = 1,2,3$ in terms of the canonical addition on $E_{k,\ell,m}$.

***Proof*** See [23], p. 51. □

The above result was derived in [23] as a special case of a general construction which yields a rationally defined isomorphism from a given rationally defined smooth intersection $Q$ of two quadrics in projective three-space to an elliptic curve in Weierstraß form which maps a distinguished rational point on $Q$ to the point at infinity. As was pointed out to us by Joseph Lipman (personal communication, July 1, 2019), such an isomorphism can also be constructed by a method described in [46], Chapter II, Appendix III which differs from the one used in [23]. We emphasize that for the purposes of this paper we need not just the abstract existence of such an isomorphism, but a concrete formula which allows us to calculate the images of any rational points which can be identified on $Q$, and the isomorphism $\Phi$ constructed in [23] yields the values given in Theorem 1. In particular, the four points $P_4, P_5, P_6, P_7$ must have either finite order greater than two or infinite order. As observed before, if one of these four points is fixed, the three other ones are obtained by adding to this point the points of order two, which implies that the subgroup of the Mordell-Weil group of $E_{k,\ell,m}$ generated by the eight points (14) is at most of rank one.

Now a deep theorem of Mazur (see [31]) states that the torsion subgroup of an arbitrary elliptic curve over $\mathbb{Q}$ can only be $\mathbb{Z}_m$ where $1 \le m \le 12$ and $m \ne 11$ or else $\mathbb{Z}_2 \times \mathbb{Z}_{2n}$ where $1 \le n \le 4$. Thus in our situation only the four latter groups can occur as the torsion subgroup $T_{k,\ell,m}$ of the Mordell-Weil group of $E_{k,\ell,m}$. This

puts us into a win-win situation: In almost any possible scenario, we can obtain a nontrivial result.

- If $T = \mathbb{Z}_2 \times \mathbb{Z}_2$, the four points $P_i$ where $4 \le i \le 7$ must necessarily have infinite order, so that $E_{k,\ell,m}$ has positive rank. This establishes the positivity of the Mordell-Weil rank for a wide class of elliptic curves by a trivial counting argument. (This argument requires only the mere existence of a rationally defined isomorphism $\Phi : Q_{k,\ell,m} \to E_{k,\ell,m}$ and not the special form of such an isomorphism.)
- If $T = \mathbb{Z}_2 \times \mathbb{Z}_{2n}$ where $2 \le n \le 4$ and if at least one of the points $P_i$ where $4 \le i \le 7$ (or a negative of such a point or a sum of such points) happens to be not one of the torsion points (which can be explicitly listed), then we can again conclude that the rank of $E_{k,\ell,m}$ is positive, this time using the explicit form of the isomorphism $\Phi : Q_{k,\ell,m} \to E_{k,\ell,m}$ (and not merely the existence of such an isomorphism).
- If $T = \mathbb{Z}_2 \times \mathbb{Z}_{2n}$ where $n = 3$ or $n = 4$, there are more than the eight torsion points identified in (14). The extraneous torsion points correspond to points on $Q_{k,\ell,m}$ other than the trivial points $(1, \pm 1, \pm 1, \pm 1)$ and hence are associated with nontrivial progressions of type $(k, \ell, m)$ or $(m, \ell, k)$. This argument establishes the existence of such progressions.

To carry out this line of reasoning, we need to identify the torsion points of an elliptic curve of the type considered, which can be easily done.

**Theorem 2** Consider the Mordell-Weil group of the elliptic curve given by the affine equation $y^2 = x(x + r)(x + s)$ where $0 < r < s$ are integers. Then the following statements hold.

(1) There are points of order 4 if and only if $r$ and $s$ are squares, say $r = u^2$ and $s = v^2$.
(2) There are points of order 8 if and only if there are numbers $a, b \in \mathbb{N}$ for which $a^2 + b^2$ is a square, say $a^2 + b^2 = c^2$, such that $r = a^4$ and $s = b^4$.
(3) There are points of order 3 (or, equivalently, points of order 6) if and only if there are coprime integers $0 < \alpha < \beta$ such that $r = \alpha^3(\alpha + 2\beta)$ and $s = \beta^3(\beta + 2\alpha)$.
(4) In all other cases, the only torsion points are the points of order 2, namely (0,0), $(-r, 0)$ and $(-s, 0)$.

***Proof*** See [32] and also [37] where, however, a different sign convention was used. □

As an immediate consequence, we can exhibit a rather large class of elliptic curves with positive Mordell-Weil rank (and explicitly identify elements of infinite order on these curves).

**Theorem 3** Assume that $(k, \ell, m)$ is a triplet such that $T_{k,\ell,m} = \mathbb{Z}_2 \times \mathbb{Z}_2$. Then necessarily $k \ne m$, and $E_{k,\ell,m}$ has positive rank. As a consequence, there are nontrivial progressions of type $(k, \ell, m)$ or $(m, \ell, k)$.

***Proof*** We must have $k \neq m$ because otherwise we would be in case (1) of Theorem 2. Since the Mordell-Weil group of $E_{k,\ell,m}$ contains only four torsion points, the points $P_4, P_5, P_6, P_7$ must have infinite order, which already yields the statement concerning the rank. Moreover, since $k \neq m$, no two of these points $P_4, P_5, P_6, P_7$ have the same $x$-coordinates, which implies that if $P$ is any of these four points, its negative $-P$ is not again one of them and hence corresponds to a nontrivial point of $Q_{k,\ell,m}$ under the isomorphism used in Theorem 1 and consequently to a nontrivial progression of type $(k, \ell, m)$ or $(m, \ell, k)$. □

***Example 1*** The case considered in the above theorem is the generic one, as a torsion group $\mathbb{Z}_2 \times \mathbb{Z}_{2n}$ with $n \geq 2$ only occurs if $k, \ell, m$ satisfy special conditions. For example, let $(k, \ell, m) = (2, 3, 5)$. The isomorphism $\Phi$ used in Theorem 1 maps the trivial points $(1, \pm 1, \pm 1, \pm 1)$ on $Q_{2,3,5}$ to the 2-torsion points and additionally to the points $P_4 = (40, 400)$, $P_5 = (10, -100)$, $P_6 = (-25, -75)$ and $P_7 = (-16, 48)$ in $E_{2,3,5}$, and these latter points have infinite order. The negative of each of these points gives rise to a nontrivial arithmetic progression. Let us take the point $P = (10, 100)$. Then $\Phi^{-1}$ maps $P$ to the point $(73, 109, 31, -151)$ on the quadric intersection $Q_{2,3,5}$, and this point corresponds to a sequence of four squares of type $(2, 3, 5)$, namely

$$31^2 < 73^2 < 109^2 < 151^2.$$

The other points yield the same sequence of squares. The point $2P$ (i.e., $P + P$ in the sense of the group law of $E_{2,3,5}$) is given by $(9/4, -273/8)$, which is mapped to the point $(808\,345, 639\,829, -903\,391, 51\,449)$ on $Q_{2,3,5}$. This point gives rise to a sequence of squares of type $(5, 3, 2)$, namely

$$51\,449^2 < 639\,829^2 < 808\,345^2 < 903\,391^2.$$

### 3.1 The case $k = m$

To further exploit these results, we first dispose of the case $k = m$. (We note that if $k = m$ then the construction of the isomorphism $\Phi$ used in Theorem 1 is considerably simpler than in the case $k \neq m$; see [23].) If $k = m$, the equation $y^2 = x(x + km)(x + (k+\ell)(\ell+m))$ becomes $y^2 = x(x + r)(x + s)$ where $r := k^2$ and $s := (k + \ell)^2$ both are squares, and one readily checks by explicitly listing the torsion points of this curve that in this case the points $P_i$ where $4 \leq i \leq 7$ are exactly the points of order four. This gives rise to the following result.

**Theorem 4** Let $k$ and $\ell$ be natural numbers. If there is a Pythagorean triplet $(a, b, c)$ with $a < b < c$ such that $k = a^2$ and $\ell = b^2 - a^2$, then $T_{k,\ell,k} = \mathbb{Z}_2 \times \mathbb{Z}_8$, and there is a nontrivial progression of type $(k, \ell, k)$, namely $0^2 < a^2 < b^2 < c^2$, and if the rank of $E_{k,\ell,k}$ is zero, there are no other nontrivial progressions. In all other cases, we have $T_{k,\ell,k} = \mathbb{Z}_2 \times \mathbb{Z}_4$, and then a nontrivial progression of type $(k, \ell, k)$ exists if and only if $E_{k,\ell,k}$ has positive rank.

***Proof*** Clearly, if $k = m$ then we are in case (1) of Theorem 2, so that $T_{k,\ell,k}$ contains $\mathbb{Z}_2 \times \mathbb{Z}_4$. We are in case (2) if and only if $k$, $k+\ell$ and $2k+\ell$ are all squares. If this is the case, say with $k = a^2$, $k+\ell = b^2$ and $2k+\ell = c^2$, then $b^2 - a^2 = \ell = c^2 - 2a^2$ and hence $a^2 + b^2 = c^2$, so that $(a, b, c)$ is a Pythagorean triplet with $a < b < c$. Conversely, given such a triplet, we let $k := m := a^2$ and $\ell := b^2 - a^2$ to be in the situation of case (2) of Theorem 2. As observed before, the four points $P_i$ where $4 \le i \le 7$ are exactly the points of order 4. Hence if $T_{k,\ell,k} = \mathbb{Z}_2 \times \mathbb{Z}_4$, the trivial points on $Q_{k,\ell,k}$ correspond exactly to the torsion points of the Mordell-Weil group of $E_{k,\ell,k}$, so that in this case nontrivial progressions of type $(k, \ell, k)$ exist exactly if the rank of $E_{k,\ell,k}$ is positive. On the other hand, if $T_{k,\ell,k} = \mathbb{Z}_2 \times \mathbb{Z}_8$ each of the points of order 8 corresponds to a nontrivial progression of type $(k, \ell, k)$. Applying the inverse of the isomorphism $\Phi$ used in Theorem 1 (see [23], pp. 50/51), one readily checks that the eight points of order 8 on $E_{k,\ell,k}$ correspond exactly to the four points $(a^2, \pm b^2, 0, \pm c^2)$ and the four points $(b^2, \pm a^2, \pm c^2, 0)$ on $Q_{k,\ell,k}$ which, in turn, all yield the progression $0^2 < a^2 < b^2 < c^2$. Clearly, if the rank of $E_{k,\ell,k}$ is zero, there are no other rational points on $E_{k,\ell,k}$, hence no other rational points on $Q_{k,\ell,k}$, and hence no other nontrivial progressions of type $(k, \ell, k)$. □

***Remark 1*** If $k = m$ and $T_{k,\ell,m} = \mathbb{Z}_2 \times \mathbb{Z}_4$, then both possibilities mentioned in the above theorem can actually occur. For example, there is no nontrivial progression of type $(1, 1, 1)$, this being Fermat's classical result, which implies that the rank of $E_{1,1,1}$ is zero, so that the only rational points on $E_{1,1,1}$ are the torsion points. On the other hand, the Mordell-Weil group of $E_{1,6,1}$ has positive rank; an element of infinite order is given by (1,10), and an associated progression of type $(1, 6, 1)$ is $1^2 < 11^2 < 29^2 < 31^2$, i.e., $1 < 121 < 841 < 961$. (The points of order 4 in this example are $(7, \pm 56)$ and $(-7, \pm 42)$, and the rank of $E_{1,6,1}$ is one.) It turns out that curves of higher rank also occur in this way; for example, the rank of $E_{1,40,1}$ equals two.

### 3.2 The case $k \neq m$

Interestingly, there are also triplets $(k, \ell, m)$ with $T_{k,\ell,m} \supseteq \mathbb{Z}_2 \times \mathbb{Z}_4$ and $k \neq m$, because both $km$ and $(k+\ell)(\ell+m)$ can be squares even if $k \neq m$. This happens if and only if we have $k = ga^2$ and $m = gb^2$, where $g \in \mathbb{N}$ is square-free and where $a^2 \neq b^2$, and if, in addition, there is a number $v$ such that $v^2 = (k+\ell)(\ell+m) = \ell^2 + (k+m)\ell + km = \ell^2 + g(a^2+b^2)\ell + g^2a^2b^2$, which, using the solution formula for quadratic equations, means that

$$\begin{aligned}
&\ell^2 + g(a^2+b^2)\ell + g^2a^2b^2 - v^2 = 0, \text{ i.e.,}\\
&2\ell = -g(a^2+b^2) + \sqrt{g^2(a^2-b^2)^2 + 4v^2}, \text{ i.e.,}\\
&(2\ell + g(a^2+b^2))^2 = (g(a^2-b^2))^2 + (2v)^2, \text{ i.e.,}\\
&(g|a^2-b^2|,\ 2v,\ 2\ell + g(a^2+b^2)) \text{ is a Pythagorean triplet.}
\end{aligned} \tag{15}$$

Note that this yields a way of constructing triplets $(k, \ell, m)$ with $k \neq m$ for which the Mordell-Weil group of $E_{k,\ell,m}$ contains points of order four, starting with a square-free number $g \in \mathbb{N}$ and then choosing two natural numbers $a \neq b$ appropriately. Choosing especially Pythagorean triplets of the form $(r^2-s^2, 2rs, r^2+s^2)$ (which comprise all primitive ones), we obtain the following result.

**Theorem 5** Given a square-free number $g \in \mathbb{N}$ and natural numbers $a \neq b$, assume that there are natural numbers $r, s \in \mathbb{N}$ such that $g(a^2 - b^2) = r^2 - s^2$ and such that $r^2 + s^2 - g(a^2 + b^2)$ is positive and even. Then a triplet $(k, \ell, m)$ with $k \neq m$ for which $T_{k,\ell,m} \supseteq \mathbb{Z}_2 \times \mathbb{Z}_4$ is given by

$$k := ga^2, \quad m := gb^2, \quad \ell := (r^2 + s^2 - g(a^2 + b^2))/2. \tag{16}$$

***Proof*** The assumptions imply that $km = (ga^2)(gb^2) = (gab)^2$ and

$$\begin{aligned}(k+\ell)(\ell+m) &= \frac{r^2+s^2+g(a^2-b^2)}{2} \cdot \frac{r^2+s^2-g(a^2-b^2)}{2} \\ &= \frac{(r^2+s^2)^2 - g^2(a^2-b^2)^2}{4} = \frac{(r^2+s^2)^2-(r^2-s^2)^2}{4} = (rs)^2\end{aligned} \tag{17}$$

are both squares, so that we are in case (1) of Theorem 2. □

***Remark 2*** The assumptions of the last theorem are satisfied in a variety of different situations.

- Assume that $g = 1$ and that $n \in \mathbb{N}$ is a natural number which has two different factorizations into factors of equal parity. This amounts to having two different representations $n = (a-b)(a+b) = (r-s)(r+s)$, i.e., $a^2 - b^2 = r^2 - s^2$, and if $r^2 + s^2 > a^2 + b^2$ then Theorem 5 is applicable. Specific examples are given by $n = 15 = 8^2 - 7^2 = 4^2 - 1^2$ with $(a, b) = (4,1)$ and $(r, s) = (8,7)$ and by $n = 48 = 8^2 - 4^2 = 7^2 - 1^2$ with $(a, b) = (7,1)$ and $(r, s) = (8,4)$.
- Assume that $g = 2G + 1$ is odd and that $a > b$ are arbitrary. Then we have $(a^2 - b^2)g = (a^2 - b^2)((G+1)^2 - G^2) = r^2 - s^2$ where $r := a(G+1) + bG$ and $s := aG + b(G+1)$, this being a special case of the identity $(a^2 - b^2)(c^2 - d^2) = (ac + bd)^2 - (ad + bc)^2$. Now a straightforward calculation shows that $r^2 + s^2 - g(a^2 + b^2)$ equals $2G(a^2 + 4ab + b^2)$ and hence is both positive and even, so that Theorem 5 is applicable.
- Assume that $g = 2G$ where $G$ is odd and that $a > b$ are both even, say $a = 2A$ and $b = 2B$. Then $(a^2-b^2)g = 8G(A^2-B^2) = r^2-s^2$ where $r := A(2G+1) + B(2G-1)$ and $s := B(2G+1) + A(2G-1)$. A straightforward calculation shows that $r^2+s^2-g(a^2+b^2)$ equals $(A^2+B^2)(8G^2-8G+2) + 4AB(2G+1)(2G-1)$ and hence is both positive and even, so that Theorem 5 is applicable.
- Assume that $g = 2G$ where $G$ is odd and that $a > b$ are both odd, say $a = 2A+1$ and $b = 2B + 1$. Letting $\alpha := A(A+1)/2$ and $\beta := B(B+1)/2$, we have $(a^2-b^2)g = 16G(\alpha-\beta) = r^2-s^2$ where $r := (G+1)(\alpha-\beta+1) + (G-1)(\alpha-\beta-1)$ and $s := (G+1)(\alpha-\beta-1) + (G-1)(\alpha-\beta+1)$. A straightforward calculation

shows that $r^2+s^2-g(a^2+b^2)$ equals $8G^2(\alpha-\beta)^2-4G(4\alpha+4\beta+1)+8$, which is even and is also positive provided that $G, A, B$ are chosen such that either $G > 4\alpha+4\beta+1+\sqrt{(8\alpha+1)(8\beta+1)}$ or else $G < 4\alpha+4\beta+1-\sqrt{(8\alpha+1)(8\beta+1)}$, in which case Theorem 5 is applicable.

Let us note that if $T_{k,\ell,m} = \mathbb{Z}_2 \times \mathbb{Z}_4$ where $k \neq m$ then the Mordell-Weil rank of $E_{k,\ell,m}$ is necessarily positive. The argument used in the proof is a slight variation of the one used to prove Theorem 3, this time however using the specific form of the isomorphism $\Phi$ and not just the mere existence of such an isomorphism.

**Theorem 6** Assume that $(k,\ell,m)$ is a triplet with $k \neq m$ such that $T_{k,\ell,m} = \mathbb{Z}_2 \times \mathbb{Z}_4$. Then the four points $P_i$ where $4 \leq i \leq 7$ all have infinite order; in particular, the rank of $E_{k,\ell,m}$ is positive. As a consequence, there are nontrivial progressions of type $(k,\ell,m)$ or $(m,\ell,k)$.

***Proof*** The four points $P_i$ where $4 \leq i \leq 7$ are either all of order four or all of infinite order. Let $P = (x,y)$ be one of these points. If $P$ had order 4, then its negative $-P = (x,-y)$ would also be of order 4 and hence would have to be again one of these four points. But this is impossible because, since $k \neq m$, no two of these points have the same $x$-coordinates. This shows that $P$ has infinite order. Now let $\Phi$ be the isomorphism used in Theorem 1. Since $-P$ is not one of the points $P_i$ where $4 \leq i \leq 7$, the inverse image $\Phi^{-1}(-P)$ is not one of the trivial points in $Q_{k,\ell,m}$ and hence belongs to a nontrivial progression of type $(k,\ell,m)$ or $(m,\ell,k)$. □

***Example 2*** If we choose $g = 1$, $(a,b) = (5,1)$ and $(r,s) = (7,5)$ in Remark 2, we get the triplet $(k,\ell,m) = (25,24,1)$ and find $P_4 = (25,1250)$, $P_5 = (1225,61250)$, $P_6 = (-49,-1176)$ and $P_7 = (-625,15000)$. Each of these points, say $P$, yields a progression of type $(1,24,25)$, namely $119^2 < 193^2 < 769^2 < 1081^2$. Amongst the points $kP$ with $k \in \mathbb{N}$, the first one to yield a progression of inverse type $(25,24,1)$ is $5P$, with the progression

$$2197483189757519^2 < 3160298284778881^2$$
$$< 3865190294552833^2 < 3891791120844719^2.$$

Note that in this example (as in many others) nontrivial progressions of both types $(k,\ell,m)$ and $(m,\ell,k)$ exist, but we do not see a general pattern which would allow us to decide which rational points on the curve $E_{k,\ell,m} = E_{m,\ell,k}$ belong to which of the two types.

***Remark 3*** In the situation of Theorem 5 we considered triplets $(k,\ell,m)$ with $k \neq m$ for which $km$ and $(k+\ell)(\ell+m)$ both are squares, say $km = u^2$ and $(k+\ell)(\ell+m) = v^2$. In this situation the underlying elliptic curve can also be realized by a triplet $(k_0,\ell_0,m_0)$ with $k_0 = m_0$, namely $(k_0,\ell_0,m_0) = (u,v-u,u)$. For such a triplet, our methods do not allow us to directly find an associated nontrivial progression. However, a rather bizarre method can be used to find such a progression,

as follows: Find a nontrivial rational point on the underlying curve by realizing this curve as $E_{k,\ell,m}$, and then apply the mapping $\Phi^{-1}$ to this point where $\Phi$ is the isomorphism associated with the realization $E_{k_0,\ell_0,m_0}$. For example, we have $E_{25,24,1} = E_{5,30,5}$. The point $P = (1, -10)$ obtained from the realization $E_{25,24,1}$ also yields a progression of type $(5, 30, 5)$, namely $1^2 < 11^2 < 29^2 < 31^2$ with step size $s = 24$. Thus if an elliptic curve can be realized by two different triplets $(k, \ell, m)$ and $(k_0, \ell_0, m_0)$, information obtained on progressions of type $(k, \ell, m)$ can be used to obtain information on progressions of type $(k_0, \ell_0, m_0)$, and vice versa.

**Theorem 7** Assume that $(k, \ell, m)$ is a triplet with $k \neq m$ such that $T_{k,\ell,m} = \mathbb{Z}_2 \times \mathbb{Z}_8$. Then there is at least one nontrivial progression of type $(k, \ell, m)$ or $(m, \ell, k)$. If the rank of $E_{k,\ell,m}$ is zero, there is only one such progression.

***Proof*** Each of the eight points of order 8 corresponds to a nontrivial point on $Q_{k,\ell,m}$ and hence to a nontrivial progression of type $(k, \ell, m)$ or $(m, \ell, k)$. Since any two points of order 8 differ only by a point of order 2 or 4, these eight points all correspond to the same progression. (This can be verified by explicitly applying the inverse of the isomorphism $\Phi$ used in Theorem 1.) The last statement is clear. □

***Remark 4*** We present here an infinite family of curves $E_{k,\ell,m}$ with $k \neq m$ and $T_{k,\ell,m} = \mathbb{Z}_2 \times \mathbb{Z}_8$, as follows: Choose any (square-free) odd number $g > 1$ and let

$$k := g, \quad \ell := \frac{g^2+1}{2} \cdot \left( \frac{g^2-1}{2} - g \right), \quad m := g^3. \tag{18}$$

A straightforward calculation shows that $km = g^4$ and $(k + \ell)(\ell + m) = ((g^2 - 1)/2)^4$ are both fourth powers and that $(g, (g^2 - 1)/2, (g^2 + 1)/2)$ is a Pythagorean triplet; hence case (2) of Theorem 2 implies that $T_{k,\ell,m} = \mathbb{Z}_2 \times \mathbb{Z}_8$. (Finding these examples is not as easy as the simple verification might suggest.) The arithmetic progression associated with a point of order 8 is found to be

$$\left(\frac{g-1}{2}\right)^2 < \left(\frac{g+1}{2}\right)^2 < \left(\frac{g(g-1)}{2}\right)^2 < \left(\frac{g(g+1)}{2}\right)^2. \tag{19}$$

For $g = 3$ we get $(k, \ell, m) = (3, 5, 27)$, and $E_{3,5,27}$ is a curve of rank zero. For $g = 15$ we get $(k, \ell, m) = (15, 10961, 3375)$, and in this case $E_{k,\ell,m}$ has rank one. For $g = 17$ we get $(k, \ell, m) = (17, 18415, 4913)$, and in this case $E_{k,\ell,m}$ has rank two.

***Remark 5*** In Remark 4, the same curve $y^2 = x(x+km)(x+(k+\ell)(\ell+m))$ can be realized by two different triplets $(k, \ell, m)$, one with $k = m$ and one with $k \neq m$. For example, $E_{3,5,27} = E_{9,7,9}$ is given by the equation $y^2 = x(x + 81)(x + 256)$, and this curve has torsion subgroup $\mathbb{Z}_2 \times \mathbb{Z}_8$ and rank zero. According to Theorem 7, there is a nontrivial progression of type $(3, 5, 27)$ (namely $1^2 < 2^2 < 3^2 < 6^2$), but

there is no nontrivial progression of type $(27, 5, 3)$. The realization $E_{9,7,9}$ of this curve is associated with the progression $0^2 < 3^2 < 4^2 < 5^2$.

There is also one case in which the existence of nontrivial progressions of type $(k, \ell, m)$ can be readily established by showing that $T_{k,\ell,m}$ contains elements of orders 3 and 6. Namely, the equations $km = \alpha^3(\alpha + 2\beta)$ and $(k + \ell)(\ell + m) = \beta^3(\beta + 2\alpha)$ as given in part (3) of Theorem 2 are satisfied if $k = \alpha^2$, $\ell = \beta^2 - \alpha^2$ and $m = \alpha(\alpha + 2\beta)$. This gives rise to the following result.

**Theorem 8** Given natural numbers $\alpha < \beta$, let

$$k := \alpha^2, \quad \ell := \beta^2 - \alpha^2, \quad m := \alpha(\alpha + 2\beta). \tag{20}$$

Then $T_{k,\ell,m} = \mathbb{Z}_2 \times \mathbb{Z}_6$, and there is a nontrivial progression of type $(k, \ell, m)$, namely $0^2 < \alpha^2 < \beta^2 < (\alpha + \beta)^2$. If the rank of $E_{k,\ell,m}$ is zero, this is the only such progression, and there is no nontrivial progression of type $(m, \ell, k)$.

***Proof*** From (20) we find that $k + \ell = \beta^2$, $\ell + m = \beta(\beta + 2\alpha)$ and $k + \ell + m = (\alpha + \beta)^2$, which allows us to express the points $P_4$, $P_5$, $P_6$, $P_7$ in terms of $\alpha$ and $\beta$. Since $r := km = \alpha^3(\alpha+2\beta)$ and $s := (k+\ell)(\ell+m) = \beta^3(\beta+2\alpha)$, we are in case (3) of Theorem 2. Explicitly writing down the torsion points in this case, we see that the points $P_4$, $P_5$, $P_6$, $P_7$ are exactly the points of the form $A + X$ where $A$ is a point of order 3 and where $X$ runs through the points of order 2. This leaves four points unaccounted for (namely the points $B + X$ where $B$ is the other point of order 3 and where $X$ runs through the point of order 2), and these points correspond to nontrivial points of $Q_{k,\ell,m}$ and hence nontrivial progressions of type $(k, \ell, m)$ or $(m, \ell, k)$. Applying the inverse of the isomorphism $\Phi$ used in Theorem 1 (see [23], pp. 50/51), one readily checks that the corresponding points on the quadric intersection $Q_{k,\ell,m}$ are the four points $(X_0, X_1, X_2, X_3) = (\pm\alpha, \pm\beta, 0, \alpha + \beta)$, which all belong to the progression $0^2 < \alpha^2 < \beta^2 < (\alpha + \beta)^2$. If the rank of $E_{k,\ell,m}$ is zero, there are no rational points on $E_{k,\ell,m}$ and hence no rational points on $Q_{k,\ell,m}$ other than the ones discussed so far, which implies that there are no additional progressions of type $(k, \ell, m)$ or $(m, \ell, k)$. □

***Remark 6*** Assume that $0 < r < s$ are such that there are integers $0 < \alpha < \beta$ with $r = \alpha^3(\alpha + 2\beta)$ and $s = \beta^3(2\alpha + \beta)$. Then Theorem 8 shows that there is a "standard triplet" $(k_0, \ell_0, m_0)$ such that the elliptic curve $E^{r,s}$ given by the equation $y^2 = x(x + r)(x + s)$ can be realized as one of the curves $E_{k,\ell,m}$, namely (20). However, in some cases there is also a different triplet $(k, \ell, m)$ realizing the same curve, which means that $km = k_0m_0 = \alpha^3(\alpha + 2\beta)$ and $(k + \ell)(\ell + m) = (k_0 + \ell_0)(\ell_0 + m_0) = \beta^3(2\alpha + \beta)$; this is, for example, the case if $(\alpha, \beta)$ is one of the pairs (3, 5), (5, 13), (5, 16), (7, 8), (8, 13) and (9, 26).

To illustrate this last remark, we discuss two cases in detail.

***Example 3*** Let $(\alpha, \beta) = (3, 5)$ so that $(r, s) = (351, 1375)$. A nonstandard triplet is given by $(k, \ell, m) = (3, 8, 117)$. For this triplet, we find $P_4 = (14625, 1872000)$, $P_5 = (33, -4224)$, $P_6 = (-1287, -10296)$ and $P_7 = (-375, 3000)$. Let $P := (33, -4224)$; then the progression of type $(3, 8, 117)$ associated with $-P$ is

$$134^2 < 151^2 < 189^2 < 474^2$$

with step size $s = 1615$. Amongst the points $kP$ where $k \in \mathbb{N}$, the first one to yield a progression of inverse type $(117, 8, 3)$ is obtained for $k = 8$, and the resulting progression is

$$\begin{aligned}
&2476701942847408549859902171636295070684368351458513 8^2 \\
&< 3375028738129833515241298833555957606269532819622203 3^2 \\
&< 3427864642420654844664538690619443767416346390485201 3^2 \\
&< 3447469345852254164582900739978533929526649385843848 2^2
\end{aligned}$$

with step size

$$\begin{aligned}
s = {} & 4492962794442844587416920986201250374115324324328646109 4/ \\
& 6564083191821402558280919800693924155864943738 5.
\end{aligned}$$

For the standard triplet $(k_0, \ell_0, m_0) = (9, 16, 39)$ we find the points $P_4 = (2145, 137280)$, $P_5 = (225, -14400)$, $P_6 = (-975, -15600)$ and $P_7 = (-495, 7920)$, and the progression of type $(9, 16, 39)$ associated with each of these four points is $0^2 < 3^2 < 5^2 < 8^2$ with step size $s = 1$. Since these points are torsion points, they cannot be used to find a progression of inverse type $(39, 16, 9)$. However, the point $P = (33, -4224)$ obtained above for the nonstandard triplet yields the progression $2^2 < 11^2 < 13^2 < 14^2$ which is of type $(39, 16, 9)$ with step size $s = 3$. The point $-P$ yields the progression $9^2 < 12^2 < 16^2 < 23^2$ with step size $s = 7$, which is of type $(9, 16, 36)$ and does not start with zero.

***Example 4*** Let $(\alpha, \beta) = (9,26)$ so that $(r, s) = (44469, 773344)$. A nonstandard triplet is given by $(k, \ell, m) = (3, 49, 14823)$. For this triplet, we find that $P_4 = (220447656, 3279158883000)$, $P_5 = (156, -2320500)$, $P_6 = (-770796, -37769004)$ and $P_7 = (-44616, 2186184)$. Let $P := P_5$; then the progression of type $(3, 49, 14823)$ associated with $-P$ is

$$50282^2 < 50323^2 < 50988^2 < 151593^2$$

with step size $s = 1374935$. Amongst the points $kP$ where $k \in \mathbb{N}$, the first one to yield a progression of inverse type $(14823, 49, 3)$ is obtained for $k = 48$, and each of the terms of this progression has more than 5000 decimal places. For the standard triplet $(k_0, \ell_0, m_0) = (81, 595, 549)$ we find $P_4 = (628056, 769368600)$, $P_5 = (54756, -67076100)$, $P_6 = (-371124, -220818780)$ and $P_7 = (-92664, 55135080)$, and the progression of type $(81, 595, 549)$ associated with each of these four points is $0^2 < 9^2 < 26^2 < 35^2$ with step size

$s = 1$. Since the points $P_i$ where $4 \leq i \leq 7$ are torsion points, they cannot be used to find a progression of inverse type $(549, 595, 81)$. However, the point $P = (156, -2320500)$ obtained above for the nonstandard triplet yields the progression $263^2 < 286^2 < 309^2 < 312^2$ which is of type $(549, 595, 81)$ with step size $s = 23$. The point $-P$ yields the progression $161^2 < 163^2 < 177^2 < 189^2$ with step size $s = 8$, which is of type $(81, 595, 549)$ and does not start with zero.

***Remark 7*** For the examples discussed in the previous remark, we are in the same situation as in Remark 3: We have two realizations of the same elliptic curve in terms of two different triplets, namely the triplet $(k, \ell, m)$ as given in the previous remark and the standard triplet $(k_0, \ell_0, m_0)$ given by $k_0 = \alpha^2$, $\ell_0 = \beta^2 - \alpha^2$ and $m_0 = \alpha(\alpha + 2\beta)$ as in Theorem 8. As in Remark 3, we can use points obtained for one triplet to find progressions for the other triplet. As an example, let us consider the case $(\alpha, \beta) = (3,5)$ with $(r, s) = (351,1375)$. Using the point $P := (33, -4224)$ (which generates the free part of $E_{3,8,117}$), we find the progression

$$134^2 < 151^2 < 189^2 < 474^2$$

with step size $s = 1615$ of type $(3, 8, 117)$. On the other hand, the nontrivial progression $0^2 < 3^2 < 5^2 < 8^2$ of type $(9, 16, 39)$ is associated with the point $Q := (2145, 137280)$, and this point yields the progression

$$4^2 < 5^2 < 7^2 < 20^2$$

with step size $s = 3$ of type $(3, 8, 117)$. In this case the negative point $-Q = (2145, -137280)$ yields the progression $2^2 < 5^2 < 9^2 < 30^2$ with step size $s = 7$, which is of the same type $(3, 8, 117)$.

## 4 The family of elliptic curves associated with the problem of four rational squares in an arithmetic progression

Up to this point, the focus of this paper was on properties of a fixed elliptic curve $E_{k,\ell,m}$ for a given triplet $(k, \ell, m)$. We now want to say something about the family of all such curves within the larger class of all curves $E^{r,s}$ for $0 < r < s$, where $E^{r,s}$ denotes the elliptic curve with the Weierstraß equation $y^2 = x(x + r)(x + s)$, and about the number of quadric intersections yielding the same elliptic curve. It is clear that for most pairs $(r, s)$ there are no triplets $(k, \ell, m)$ with $E_{k,\ell,m} = E^{r,s}$, for many pairs $(r, s)$ there is exactly one triplet $(k, \ell, m)$ with $k \leq m$ such that $E_{k,\ell,m} = E^{r,s}$ and for some pairs $(r, s)$ there is more than one triplet $(k, \ell, m)$ with $k \leq m$ such that $E_{k,\ell,m} = E^{r,s}$. We now show in general that a given curve $E^{r,s}$ can only be realized in finitely many ways as a curve $E_{k,\ell,m}$ and hence as a quadric intersection.

**Theorem 9** For each pair $(r, s)$ with $0 < r < s$, the number of triplets $(k, \ell, m)$ for which $E_{k,\ell,m} = E^{r,s}$ is finite. At least one such triplet exists whenever the torsion group of the Mordell-Weil group of $E^{r,s}$ is strictly larger than $\mathbb{Z}_2 \times \mathbb{Z}_2$.

***Proof*** If the equations $r = km$ and $s = (k + \ell)(\ell + m)$ are to hold, then $k$ must be a divisor of $r$, and $m$ is uniquely determined by $k$. Moreover, given $k$ and $m$, there can be at most one number $\ell$ satisfying $s = (k + \ell)(\ell + m)$, because the mapping $\ell \mapsto (k + \ell)(\ell + m)$ is strictly increasing. Hence the number $N(r, s)$ of triplets $(k, \ell, m)$ satisfying $r = km$ and $s = (k + \ell)(\ell + m)$ cannot exceed the number $D(r)$ of divisors of $r$. Analogously, this number also cannot exceed $D(s)$. Since the roles of $k$ and $m$ can be exchanged, we even get the estimate

$$N(r,s) \le \begin{cases} (1/2) \cdot M(r,s), & \text{if neither } r \text{ nor } s \text{ is a square,} \\ (1/2) \cdot (M(r,s) + 1), & \text{if } r \text{ or } s \text{ is a square,} \end{cases} \tag{21}$$

where $M(r, s) := \min(D(r), D(s))$. This proves the first part of the claim. To prove the second part, let $T$ be the torsion group of the Mordell-Weil group of $E^{r,s}$. If $T \supseteq \mathbb{Z}_2 \times \mathbb{Z}_4$, there are integers $u$ and $v$ such that $r = u^2$ and $s = v^2$ where $0 < u < v$. Letting $k := m := u$ and $\ell := v - u$, we find that $km = u^2 = r$ and $(k + \ell)(\ell + m) = v^2 = s$ and hence $E^{r,s} = E_{k,\ell,m}$. If $T \cong \mathbb{Z}_2 \times \mathbb{Z}_6$, there are integers $0 < \alpha < \beta$ such that $r = \alpha^3(\alpha + 2\beta)$ and $s = \beta^3(\beta + 2\alpha)$. Letting $k := \alpha^2$, $\ell := \beta^2 - \alpha^2$ and $m := \alpha(\alpha + 2\beta)$, we find that $km = \alpha^3(\alpha + 2\beta) = r$ and $(k + \ell)(\ell + m) = \beta^3(\beta + 2\alpha) = s$ and hence $E^{r,s} = E_{k,\ell,m}$. □

***Remark 8*** To prove that an elliptic curve $E^{r,s}$ allows only a finite number of realizations $E_{k,\ell,m}$ we used an elementary argument tailormade for the situation. We want to point out that this fact also follows from a rather general argument. Namely, assume that we have representations $r = km$ and $s = (k + \ell)(\ell + m)$. Then $ks = (k + \ell)(k\ell + km) = (k + \ell)(k\ell + r) = k^2\ell + k\ell^2 + rk + r\ell$, which shows that $(x, y) := (k, \ell)$ is a point on the curve $C$ given by the affine equation $sx = x^2y + xy^2 + rx + ry$. Now it is readily checked that $C$ is a smooth cubic; hence by Siegel's Theorem (cf. [38], Chap. 5, 5.1, Theorem 5.1) the number of integral points on the curve $C$ is finite, which shows that there are only finitely many triplets $(k, \ell, m)$ with $E_{k,\ell,m} = E^{r,s}$.

***Remark 9*** The proof of the above theorem shows that if $T \supseteq \mathbb{Z}_2 \times \mathbb{Z}_4$ then $E^{r,s}$ can be realized as a curve $E_{k,\ell,m}$ with $k = m$. However, in some cases a realization with $k \neq m$ is also possible; cf. Remark 2. As a variation of the first construction in Remark 2, examples for this phenomenon can be obtained as follows: Choose a natural number $n$ which can be written in two different ways as a sum of two squares, say $n = t^2 + u^2 = v^2 + w^2$ where we may assume $0 < t < v < w < u$, and then let $k := t^2$, $m := v^2$ and $\ell := w^2 - t^2 = u^2 - v^2$. Then $km = (tv)^2 =: r$ and $(k+\ell)(\ell+m) = (wu)^2 =: s$, so that $(r, s)$ yields an example of the desired type. Similarly, if $T = \mathbb{Z}_2 \times \mathbb{Z}_6$ there are also examples of curves $E^{r,s}$ with $r = \alpha^3(\alpha+2\beta)$ and $s = \beta^3(\beta + 2\alpha)$ which can be realized as $E_{k,\ell,m}$ where $(k, \ell, m)$ differs from the triplet used in the proof of Theorem 1; see Remark 6 above.

***Remark 10*** Assume that numbers $0 < r < s$ are given and that $T$ is the torsion subgroup of the Mordell-Weil group of $E^{r,s}$. Assume that there is at least one triplet $(k, \ell, m)$ such that $r = km$ and $s = (k + \ell)(\ell + m)$ (so that $E^{r,s}$ can be realized as one of the curves $E_{k,\ell,m}$). Then our results guarantee $E^{r,s}$ to be of positive rank in each of the following cases:

- $T \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (this being the generic case);
- $T \cong \mathbb{Z}_2 \times \mathbb{Z}_4$, and there is more than one triplet $(k, \ell, m)$ such that $r = km$ and $s = (k + \ell)(\ell + m)$;
- $T \cong \mathbb{Z}_2 \times \mathbb{Z}_6$, and there is at least one triplet $(k, \ell, m)$ such that $r = km$ and $s = (k + \ell)(\ell + m)$ for which there is a torsion point on $E_{k,\ell,m}$ for which the corresponding point on $Q_{k,\ell,m}$ does not have zero as one of its entries (which means that the associated nontrivial progression of type $(k, \ell, m)$ does not start with zero).

## 5 Connections to other theories

Any rationally defined elliptic curve with torsion subgroup containing $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to a curve of type $E^{r,s}$ given by an equation of the form $y^2 = x(x + r)(x + s)$ with integers $0 < r < s$. The curves $E_{k,\ell,m}$ form only a proper subfamily of such curves. However, since the curves of type $E^{r,s}$ are strongly connected to other number-theoretical problems, our results for the curves $E_{k,\ell,m}$ have consequences for these problems.

### 5.1 The problem of concordant forms

Any of the curves $E^{r,s}$ is isomorphic to the intersection of the two quadrics in projective three-space given by $X_0^2 + rX_1^2 = X_2^2$ and $X_0^2 + sX_1^2 = X_3^2$ (see [37]) and hence is intimately related to Euler's concordant form problem described before. Our results give additional information for the special cases which correspond to the curves $E_{k,\ell,m}$. For example, if the rank of $E_{k,\ell,m}$ is zero and the torsion subgroup is either $\mathbb{Z}_2 \times \mathbb{Z}_6$ or $\mathbb{Z}_2 \times \mathbb{Z}_8$, we explicitly find the singular solutions to the concordant form problem defined by torsion points. On the other hand, if the rank of $E_{k,\ell,m}$ is positive (which, as we saw, is automatically the case if $T_{k,\ell,m} = \mathbb{Z}_2 \times \mathbb{Z}_2$ or if $T_{k,\ell,m} = \mathbb{Z}_2 \times \mathbb{Z}_4$ and $k \neq m$), then the numbers $km$ and $(k + \ell)(\ell + m)$ (or the corresponding quadratic forms $X^2 + kmY^2$ and $X^2 + (k + \ell)(\ell + m)Y^2$) are concordant in the sense of Euler. Apart from this abstract information, our calculations yield explicit nontrivial solutions of the associated equations $X^2 + kmY^2 = Z^2$ and $X^2 + (k + \ell)(\ell + m)Y^2 = W^2$, in fact, even an arbitrarily large number of essentially different such solutions.

***Example 5*** The curve $E_{2,3,5} = E^{10,40}$ with the equation $y^2 = x(x + 10)(x + 40)$ is isomorphic to the curve $E^{-10,30}$ with the equation $y^2 = x(x - 10)(x + 30)$ via the translation $x \mapsto x - 10$, and this latter curve is isomorphic to the intersection of the two quadrics given by $X_0^2 - 10X_1^2 - X_2^2 = 0$ and $X_0^2 + 30X_1^2 - X_3^2 = 0$ via the isomorphism presented in [37]. The 2-torsion points are mapped to the

trivial solutions $(1, 0, \pm 1, \pm 1)$, the point $P = (10, -100)$ is mapped to the solution $(-7, -2, 3, -13)$, the other points $(40, 400)$, $(-16, 48)$ and $(-25, -75)$ as well as their negatives yield the same solution apart from sign variations. They all lead to the sequence of squares

$$(3/2)^2 < (7/2)^2 < (13/2)^2$$

with step sizes $1 \cdot 10 = 10$ and $3 \cdot 10 = 30$. The doubled point $2P = (9/4, -273/8)$ is mapped to the point $(-7201, -1092, 6319, -9361)$, which defines the sequence of squares

$$(6319/1092)^2 < (7201/1092)^2 < (9361/1092)^2.$$

### 5.2 The problem of $\theta$-congruent numbers

Given any triplet $(k, \ell, m)$, the elliptic curve $E_{k,\ell,m}$ is (by a trivial translation $x \mapsto x + km$) isomorphic to the elliptic curve

$$y^2 = x(x - km)(x + \ell(k + \ell + m)). \tag{22}$$

Now if at least one of the numbers $k + \ell$ and $\ell + m$ is even, then the numbers $\ell(k + \ell + m) \pm km$ are both even, which means that there are a natural number $N \in \mathbb{N}$ and coprime integers $r, s \in \mathbb{Z}$ with $s > 0$ such that

$$\begin{aligned} 2Nr &= \ell(k + \ell + m) - km, \\ 2Ns &= \ell(k + \ell + m) + km = (k + \ell)(\ell + m) \end{aligned} \tag{23}$$

and hence $km = N(s - r)$ and $\ell(k + \ell + m) = N(s + r)$. Consequently, the curve (22) becomes

$$y^2 = x(x - (s - r)N)(x + (s + r)N). \tag{24}$$

Hence $E_{k,\ell,m}$ has points of order greater than two if and only if this is true for the curve (24), and this is the case if and only if $N$ is $\theta$-congruent where

$$\cos(\theta) = \frac{r}{s} = \frac{\ell(k + \ell + m) - km}{\ell(k + \ell + m) + km} \tag{25}$$

(see [10, 11]). Thus our results also have some bearing on the problem of $\theta$-congruent numbers. In addition, there is a direct connection to the existence of three rational squares in an arithmetic progression with prescribed step sizes $pn$ and $qn$ where $pn = km$ and $qn = \ell(k + \ell + m)$. Again, we can not only abstractly show that some number $N$ is $\theta$-congruent, but can explicitly construct triangles corresponding to the numbers in question.

***Example 6*** Let $(k, \ell, m) = (2, 3, 5)$. The curve $E_{2,3,5}$ is isomorphic to $E^{-10,30}$, which is exactly the elliptic curve which determines whether or not 10 is a $(\pi/3)$-congruent number. Since the rank of this curve is positive, we conclude that the number 10 is indeed $(\pi/3)$-congruent, and the solution $P = (10, 100)$ found before in Example 1 corresponds to the triangle with sides 5, 8 and 7 which has $\pi/3$ as one of its angles and $F = 10\sqrt{2^2 - 1^2}$ as its area. The doubled point $2P = (9/4, -273{,}8)$ gives rise to the $(\pi/3)$-triangle with sides 39/14, 560/39 and 7201/546 with the same area. (We note that in [48] (p. 396) the author shows numbers $n$ with $n \equiv 10$ modulo 24 to be $(\pi/3)$-congruent under the assumption of the Birch-Swinnerton-Dyer conjecture. The example studied here is a special case of this situation.)

## 6 Concluding remarks and outlook

We set out to use the theory of elliptic curves to shed some light on the number-theoretical question which progressions of four rational squares are possible. Ironically, the most remarkable results were obtained in the other direction: The mere existence of nontrivial progressions could be exploited to show a rather large class of elliptic curves to be of positive rank. The argument used is completely elementary, invoking no analytical machinery such as $L$-functions and the like, and yields an explicit construction of elements of infinite order along the way.

### 6.1 Extensions of the work

It is quite conceivable that the methods described in this paper can also be applied in similar contexts to construct elliptic curves with a preassigned minimum number of rational points, as follows. Take two rationally defined diagonal quadrics in $\mathbb{P}^3(\mathbb{C})$, depending on some parameters $k$, $\ell$, ..., whose intersection is an irreducible curve $C$ which always, i.e., independently of the parameters, contains a fixed rational point $(x_0, x_1, x_2, x_3)$ with $x_i \neq 0$ for all $i$. Then $C$ has eight *a priori* known rational points $(x_0, \pm x_1, \pm x_2, \pm x_3)$. This intersection of quadrics is isomorphic to some elliptic curve, which – by the same arguments as in our cases – has eight rational points which are known *a priori*. Then an analysis analogous to ours can be used to draw conclusions on this family of elliptic curves concerning ranks, torsion points and so on.

We can also study the intersection of more than two quadrics, as follows. Take any family of $n > 1$ rationally defined diagonal quadrics in $\mathbb{P}^{n+1}(\mathbb{C})$, depending on some parameters $k$, $\ell$, ..., whose intersection is an irreducible curve $C$ which always, i.e., independently of the parameters, contains a fixed rational point $(x_0, x_1, ..., x_{n+1})$ with $x_i \neq 0$ for all $i$. Then $C$ is isomorphic to some curve $C_{k,\ell,...}$ of genus $g > 1$. By Faltings' theorem (see [9]), the total number of rational points on any of these curves is finite, but they all have a fixed number of *a priori* known rational points $(x_0, \pm x_1, ..., \pm x_{n+1})$. This could be used as a way to construct curves with "many" rational points. For recent work in this direction see [12] and [40].

### 6.2 A conjecture

We would like to conclude this paper with a conjecture. Given a nontrivial progression of type $(k, \ell, m)$, one can ask whether or not there is also a nontrivial progression of inverse type $(m, \ell, k)$. We conjecture that the answer to this purely number-theoretical question is affirmative whenever the elliptic curve $E_{k,\ell,m}$ has positive Mordell-Weil rank, i.e., in all cases other than the ones identified in Theorem 7 and Theorem 8. We verified the validity of this conjecture in all examples we studied. However, finding progressions of inverse type turned out to be rather difficult, and it is not clear to what extent the arithmetic of the elliptic curves involved can be used to answer this question. Thus attacking the conjecture requires new ideas which are beyond the scope of the present paper.

**Funding** Open Access funding provided by Projekt DEAL.



## References

1. Anonymus: No four squares in arithmetic progression (2020). http://www.mathpages.com/home/kmath044/kmath044.htm (last accessed 23 Mar 2020)
2. Bell, E.T.: Euler's concordant forms. Proc. Natl. Acad. Sci. U. S. A. **25**, 46–48 (1939)
3. Bombieri, E., Granville, A., Pintz, J.: Squares in arithmetic progressions. https://dms.umontreal.ca/~andrew/PDF/SquaresinAPs.pdf (last accessed 23 Mar 2020)
4. Brungs, A., Mudroch, V., Schulthess, P.: 13. Jahrhundert. In: Die Philosophie des Mittelalters Grundriss der Geschichte der Philosophie, vol. 4, Schwabe, Basel (2017)
5. Campbell, G., Goins, E.H.: Heron triangles, Diophantine problems and elliptic curves. http://www.math.purdue.edu/~egoins/notes/Heron_Triangles_Diophantine_Problems_and_Elliptic_Curves.pdf (last accessed 23 Mar 2020)
6. Conrad, K.: Arithmetic progression of four squares. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/4squarearithprog.pdf (last accessed 23 Mar 2020)
7. Dickson, L.E.: Diophantine Analysis. History of the Theory of Numbers, vol. II. Carnegie Institution, Washington (1920)
8. Euler, L.: De binis formulis speciei xx+myy et xx+nyy inter se concordibus et discordibus, Mem. Acad. Sci. St.-Petersbourg, Opera Omnia: Ser. 1, Vol. 5, pp. 406–413 (1780)
9. Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent Math **73**(3), 349–366 (1983)
10. Fujiwara, M.: θ-congruent numbers. In: Györy, K. (ed.) Number Theory, pp. 235–241. de Gruyter, Berlin (1998)
11. Fujiwara, M.: Some Properties of θ-congruent Numbers. Natural Science Report, vol. 52(2). (2001). Ochanomizu University
12. Gonzáles-Jiménez, E.: Covering techniques and rational points on some genus 5 curves. In: Trends in Number Theory Contemp. Math., vol. 649, pp. 89–105. Am. Math. Soc., Providence (2015)
13. Gonzáles-Jiménez, E., Steuding, J.: Arithmetic progressions of four squares over quadratic fields. Publ. Math. Debr. **77**(1-2), 125–138 (2010)

14. Gonzáles-Jiménez, E., Xarles, X.: Five squares in arithmetic progression over quadratic fields. Rev. Ma. Iberoamericana **29**(4), 1211–1238 (2013)
15. Gonzáles-Jiménez, E., Xarles, X.: On a conjecture of Rudin on squares in arithmetic progressions. LMS J. Comput. Math. **17**(1), 58–76 (2014)
16. Heegner, K.: Diophantische Analysis and Modulfunktionen. Math. Z. **56**(3), 227–253 (1952)
17. Im, B.-H.: Concordant numbers within arithmetic progressions and elliptic curves. Proc. Am. Math. Soc. **141**(3), 791–800 (2013)
18. Itard, J.: Arithmétique et Théorie des Nombres. Presses Universitaires de Paris, Paris (1963)
19. Jacobi, C.G.J.: De usu theoriae integralium ellipticorum et integralium Abelianorum in analysi Diophantea. J. Reine Angew. Math. **13**, 353–355 (1835)
20. Janfada, A.S., Salami, S., Dujella, A., Peral, J.C.: On the high rank $\pi/3$- and $2\pi/3$-congruent number elliptic curves. Rocky Mt. J. Math. **44**(6), 1867–1880 (2014)
21. Juel, C.: Ueber die Parameterbestimmung von Punkten auf Curven zweiter und dritter Ordnung. Eine geometrische Einleitung in die Theorie der logarithmischen und elliptischen Functionen. Math. Ann. **47**, 72–104 (1896)
22. Kan, M.: $\theta$-congruent numbers and elliptic curves. Acta Arith. **94**(2), 153–160 (2000)
23. Knaf, H., Selder, E., Spindler, K.: Explicit transformation of an intersection of two quadrics to an elliptic curve in Weierstraß form (2019). arXiv:1906.10230
24. Knaf, H., Selder, E., Spindler, K.: An algorithm to find rational points on elliptic curves related to the concordant form problem (2019). arXiv:1907.02148
25. Koblitz, N.: Introduction to Elliptic Curves and Modular Forms. Springer, Berlin, Heidelberg, New York (1993)
26. Kummer, E.E.: Über die Vierecke, deren Seiten und Diagonalen rational sind. J. Reine Angew. Math. **37**, 1–20 (1848)
27. Kurz, S.: On the generation of Heronian triangles. Serdica J. Comput. **2**(2), 181–196 (2008)
28. Lagrange, J.: Nombres congruents et courbes elliptiques, Séminaire Delange–Pisot–Poitou. Théorie des nombres **16**(1), 1–17 (1975)
29. Long, L.: On Shioda-Inose structures of one-parameter families of K3 surfaces. J. Number Theory **109**(2), 299–318 (2004)
30. Lucas, E.: Recherche sur plusieurs ouvrages de Léonard de Pise. Bullettino di bibliografia e di storia delle scienze matematiche e fisiche (1877)
31. Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math. L'I.H.E.S. **47**(2), 33–186 (1977)
32. Ono, K.: Euler's concordant forms. Acta Arith. **LXXVIII**(2), 101–123 (1996)
33. Ono, T.: Variations on a Theme of Euler. Plenum Press, New York, London (1994)
34. Ouyang, Y., Zhang, S.: On non-congruent numbers with 1 modulo 4 prime factors (2012). arXiv: 1208.2149
35. Rudin, W.: Trigonometric series with gaps. J. Math. Mech. **9**(2), 203–227 (1960)
36. Selder, E., Spindler, K.: A geometric approach to Euler's addition formula. Math. Semesterber. **58**, 185–214 (2011)
37. Selder, E., Spindler, K.: On $\theta$-congruent numbers, rational squares in arithmetic progressions, concordant forms and elliptic curves. Mathematics **3**(1), 2–15 (2014)
38. Silverman, J.H., Tate, J.: Rational Points on Elliptic Curves, 2nd edn. Springer, Berlin, Heidelberg, New York (2015)
39. Smith, A.: The congruent numbers have positive natural density (2016). arXiv:1603.08479v2
40. Stoll, M.: Diagonal genus 5 curves, elliptic curves over $\mathbb{Q}(t)$, and rational Diophantic quintuples. Acta Arith. **190**(3), 239–261 (2019)
41. Tian, Y.: Congruent numbers and Heegner points. Camb. J. Math. **2**(1), 117–161 (2014)
42. Tian, Y., Yuan, X., Zhang, S.: Genus periods, genus points and congruent number problem. Asian J. Math. **21**(4), 721–774 (2017)
43. Top, J., Yui, N.: Congruent number problems and their variants. Algorithmic Number Theory **44**, 613–639 (2008)
44. Tunnell, J.B.: A classical Diophantine problem and modular forms of weight 3/2. Invent Math **72**(2), 323–334 (1983)
45. van der Poorten, A.: Fermat's four squares theorem (2007). arXiv:0712.3850
46. Weil, A.: Number Theory – An Approach through History from Hammurapi to Legendre. Birkhäuser, Boston, Basel, Berlin (2007)
47. Xarles, X.: Squares in arithmetic progression over number fields. J. Number Theory **132**(3), 379–389 (2012)
48. Yoshida, S.: Some variants of the congruent number problem I. Kyushu J. Math. **55**, 387–404 (2001)

49. Yoshida, S.: Some variants of the congruent number problem II. Kyushu J. Math. **56**, 147–165 (2002)
50. Yoshida, S.: Some Variants of the Congruent Number Problem III. Technical Report (2008). Chiba University
51. Zagier, D.: Elliptische Kurven: Fortschritte und Anwendungen. Jahresber. DMV **92**, 58–76 (1990)