ARITHMETIC PROGRESSIONS ON CONIC SECTIONS

ALEJANDRA ALVARADO* and EDRAY HERBER GOINS†

Department of Mathematics, Purdue University
150 North University Street
West Lafayette, IN 47907, USA
*alvaraa@math.purdue.edu
†egoins@math.purdue.edu

Received 24 October 2012
Accepted 25 February 2013
Published 4 July 2013

The set \{1, 25, 49\} is a 3-term collection of integers which forms an arithmetic progression of perfect squares. We view the set \{(1:1), (5:25), (7:49)\} as a 3-term collection of rational points on the parabola \(y = x^2\) whose \(y\)-coordinates form an arithmetic progression. In this exposition, we provide a generalization to 3-term arithmetic progressions on arbitrary conic sections \(C\) with respect to a linear rational map \(\ell: C \rightarrow \mathbb{P}^1\). We explain how this construction is related to rational points on the universal elliptic curve \(Y^2 + 4XY + 4Y = X^3 + kX^2\) classifying those curves possessing a rational 4-torsion point.

Keywords: Arithmetic progressions; conic sections; elliptic curves; congruent number.

Mathematics Subject Classification 2010: 11B25, 11E16, 14H52

1. Introduction

An \(n\)-term arithmetic progression is a collection of rational numbers \(\{\ell_1, \ell_2, \ldots, \ell_n\}\) such that there is a common difference \(\delta = \ell_{i+1} - \ell_i\). The set \{1, 25, 49\} is a 3-term collection of integers which forms an arithmetic progression of perfect squares. We view the set \{(1 : 1), (5 : 25 : 1), (7 : 49 : 1)\} as a 3-term collection of rational points \((x : y : 1)\) on the parabola \(y = x^2\) whose \(y\)-coordinates form an arithmetic progression. It is well-known that there are infinitely many such progressions of points on the parabola:

\[
\{P_1, P_2, P_3\} = \begin{cases} 
(t^2 - 2t - 1 : (t^2 - 2t - 1)^2 : 1), \\
(t^2 + 1 : (t^2 + 1)^2 : 1), \\
(t^2 + 2t - 1 : (t^2 + 2t - 1)^2 : 1)
\end{cases}
\]

In this article, we consider the question of forming a 3-term arithmetic progression on an arbitrary conic section.
Here is our main result. We will say that \( \{P_1, P_2, P_3\} \subseteq \mathbb{P}^2(K) \) forms an arithmetic progression on a conic section

\[
C = \{(x_1 : x_2 : x_0) \in \mathbb{P}^2 \mid Ax_1^2 + 2Bx_1x_2 + Cx_2^2 + 2Dx_1x_0 + 2Ex_2x_0 + Fx_0^2 = 0\}
\]

with respect to a linear rational map

\[
\mathcal{C}(K) \xrightarrow{\ell} \mathbb{P}^1(K), \quad \text{(x_1 : x_2 : x_0)} \mapsto \frac{ax_1 + bx_2 + cx_0}{dx_1 + ex_2 + fx_0}
\]
defined over a field \( K \) of characteristic different from 2 if there is a common difference \( \delta = \ell(P_2) - \ell(P_1) = \ell(P_3) - \ell(P_2) \). Consider those \( t_0 \in K \) such that \( \sqrt{\text{Disc}(t_0)} \in K \) and

\[
k = \frac{\text{Disc}'(t_0)^2 - 2\text{Disc}(t_0)\text{Disc}''(t_0)}{\text{Disc}'(t_0)^2} \neq 0, 1, \infty
\]
in terms of the discriminant

\[
\text{Disc}(t) = \begin{bmatrix} a - dt & b - et & c - ft \\ b - et & b - et & b - et \\ c - ft & b - et & c - ft \end{bmatrix}^T \begin{bmatrix} a - dt & b - et & c - ft \\ b - et & b - et & b - et \\ c - ft & b - et & c - ft \end{bmatrix} \begin{bmatrix} a - dt \\ b - et \\ c - ft \end{bmatrix}.
\]

For each \( K \)-rational point \( (X : Y : 1) \) on the elliptic curve

\[
E_k : Y^2 + 4XY + 4kY = X^3 + kX^2
\]

the desired set is

\[
\{P_1, P_2, P_3\} = \left\{ \begin{array}{l}
(x_1(t_0 - \delta) : x_2(t_0 - \delta) : x_0(t_0 - \delta)), \\
(x_1(t_0) : x_2(t_0) : x_0(t_0)), \\
(x_1(t_0 + \delta) : x_2(t_0 + \delta) : x_0(t_0 + \delta))
\end{array} \right\}
\]

in terms of the coordinates

\[
x_1(t) = B(b - et)(c - ft) - C(a - dt)(c - ft) - D(b - et)^2 + E(a - dt)(b - et) \pm (b - et)\sqrt{\text{Disc}(t)},
\]

\[
x_2(t) = -A(b - et)(c - ft) + B(a - dt)(c - ft) + D(a - dt)(b - et) - E(a - dt)^2 \mp (a - dt)\sqrt{\text{Disc}(t)},
\]

\[
x_0(t) = A(b - et)^2 - 2B(a - dt)(b - et) + C(a - dt)^2
\]

and the common difference is

\[
\delta = \frac{\text{Disc}(t_0)}{\text{Disc}'(t_0)} \frac{4XY}{Y^2 + 2XY + kX^2}.
\]
For example, the special case of squares in arithmetic progression follows from consideration of the parabola $C : y = x^2$ and the linear polynomial $\ell(x, y, 1) = y$, so that $\text{Disc}(t) = t$. We may choose $t_0 = 1$ to find the previously mentioned 3-term progression of squares.

The condition $\sqrt{\text{Disc}(t_0)} \in K$ is both necessary and sufficient for the existence of points $P_0 \in C(K)$ such that $\ell(P_0) = t_0$, while the condition $k \neq 0, 1, \infty$ is both necessary and sufficient for $E_k$ to be an elliptic curve. Surprisingly, this curve is universal in that it classifies those elliptic curves possessing a rational 4-torsion point.

2. Squares in Arithmetic Progression

Let $K$ be a field of characteristic different from 2, which in practice is either $\mathbb{Q}$ or a quadratic extension $\mathbb{Q}(\sqrt{k})$ thereof. We will say that a collection $\{y_1, y_2, \ldots, y_n\} \subseteq K$ is an $n$-term arithmetic progression of squares over $K$ if

(i) each $y_i = x_i^2$ for some $x_i \in K$, and

(ii) there is a common difference $\delta = y_{i+1} - y_i$.

For example, the set $\{1, 25, 49\}$ is a 3-term collection of integers which forms an arithmetic progression, where the common difference is $\delta = 24$. Most of the results which are contained in this section are well-known in the literature; see, for instance, [5, 6, 11]. We include these results in the exposition at hand in order to both include simplified proofs and motivate generalizations.

2.1. Three squares in arithmetic progression

Let us first classify the 3-term case.

**Proposition 2.1.** $\{y_1, y_2, y_3\} \subseteq K$ are three squares in an arithmetic progression if and only if there exists $t \in K$ such that

$$(y_1 : y_2 : y_3) = ((t^2 - 2t - 1)^2 : (t^2 + 1)^2 : (t^2 + 2t - 1)^2).$$

**Proof.** Set $y_1 = x_1^2$, $y_2 = x_2^2$, and $y_3 = x_3^2$. We will use the following equations:

$$\begin{align*}
  x_1^2 - 2x_2^2 + x_3^2 &= 0, \\
  x_1^2 - 2x_2^2 + x_3^2 &= t \\
  x_1 - x_3 &= t \\
  x_1 - 2x_2 + x_3 &= t \frac{t^2 - 2t - 1}{t^2 + 1},
\end{align*}$$

If the ratio $(y_1 : y_2 : y_3)$ is as above, then $\delta = 4(t^3 - t)/(t^2 + 1)^2 \cdot x_2^2$ is the common difference. Conversely, if $\{y_1, y_2, y_3\} \subseteq K$ are three squares in an arithmetic progression, then the ratio $(y_1 : y_2 : y_3)$ is as above for $t = (x_1 - x_3)/(x_1 - 2x_2 + x_3)$. $\Box$
There are only certain common differences \( \delta \) which can occur for such an arithmetic progression.

**Corollary 2.2.** The following statements are equivalent for each nonzero \( \delta \in K \).

1. There exist \( x_1, x_2, x_3 \in K \) such that \( x_2^2 - \delta = x_1^2 \) and \( x_2^2 + \delta = x_3^2 \).
2. There exist \( X, Y \in K \) with \( Y \neq 0 \) such that \( Y^2 = X^3 - 2\delta X \).
3. There exist \( a, b, c \in K \) such that \( a^2 + b^2 = c^2 \) and \( (1/2)ab = \delta \).

**Proof.** We found above that there exist \( x_1, x_2, x_3 \in K \) such that \( \delta = x_2^2 - x_1^2 = x_3^2 - x_2^2 \) if and only if \( \delta = 4(t^3 - t)/(t^2 + 1)^2 \cdot x_3^2 \) for some \( t \in K \). This motivates the following transformation:

\[
\begin{align*}
X &= \frac{(x_1 - x_3) \delta}{x_1 - 2x_2 + x_3}, \\
Y &= \frac{2\delta^2}{x_1 - 2x_2 + x_3},
\end{align*}
\]

\[
\begin{align*}
x_1 &= \frac{X^2 - 2\delta X - \delta^2}{2Y}, \\
x_2 &= \frac{X^2 + \delta^2}{2Y}, \\
x_3 &= \frac{X^2 + 2\delta X - \delta^2}{2Y}.
\end{align*}
\]

Hence \( \delta = x_2^2 - x_1^2 = x_3^2 - x_2^2 \) if and only if \( Y^2 = X^3 - 2\delta X \) for some nonzero \( Y \).

Similarly, we have the following transformation:

\[
\begin{align*}
a &= \frac{X^2 - \delta^2}{Y}, \\
b &= \frac{2\delta X}{Y}, \\
c &= \frac{X^2 + \delta^2}{Y},
\end{align*}
\]

\[
\begin{align*}
X &= \frac{b\delta}{c - a}, \\
Y &= \frac{2\delta^2}{c - a}.
\end{align*}
\]

Hence \( Y^2 = X^3 - 2\delta X \) for some nonzero \( Y \) if and only if \( a^2 + b^2 = c^2 \) and \( ab = 2\delta \).

Any nonzero \( \delta \in K \) satisfying the equivalent criteria above is called a *congruum*, or even a *congruent number*, although this notation is perhaps more standard for \( K = \mathbb{Q} \). Chandrasekar [3] and Izadi [8] have written a nice summary of the history of the problem of determining when \( \delta \in \mathbb{Z}_{>0} \) is a congruent number. This notation comes from Fibonacci’s 1225 work *Liber Quadratorum*, where he shows \( \delta = 5, 6, 7 \) are congruent numbers, although similar results appeared much earlier with Al-Karaji some 200 years before. In 1640, Fermat showed that \( \delta = 1, 2, 3, 4 \) are not congruent numbers. In 1972, Alter, Curtz, and Kubota [1] conjectured that if \( \delta \) is an integer congruent to 5, 6, 7 (mod 8) then \( \delta \) is a congruent number. In 1983, Tunnell [10] found a necessary and sufficient condition for \( \delta \) to be a congruent number and translated this into properties of the quadratic twists of the elliptic curve \( Y^2 = X^3 - X \). For example, if \( \delta \equiv 5, 6, 7 \) (mod 8) then \( Y^2 = X^3 - 2\delta X \) should have positive rank.
2.2. Four or more squares in arithmetic progression

Fermat’s work is not limited to congruent numbers. He also stated that there are no nonconstant \( n \)-term arithmetic progressions whose terms are perfect squares over \( \mathbb{Q} \) if \( n \geq 4 \). Euler gave a rigorous proof of this claim in 1780. We recast this in the modern language of elliptic curves.

**Theorem 2.3.** Let \( K \) be a field of characteristic different from 2.

1. \( \{y_1, y_2, y_3, y_4\} \subseteq K \) are four squares in an arithmetic progression if and only if the elliptic curve \( Y^2 = X^3 + 5X^2 + 4X \) has a \( K \)-rational point \( (X : Y : 1) \).

2. If point \( (X : Y : 1) \) is a \( K \)-rational point on the quadratic twist \( Y^2 = X^3 + 5kX^2 + 4k^2X \), then the following conditions are four squares in an arithmetic progression over \( K(\sqrt{k}) \):

\[
\begin{align*}
y_1 &= (3kX(2k + X) - 2\sqrt{k}Y(2k - X))^2, \\
y_2 &= (kX(2k - X) - 2\sqrt{k}Y(2k + X))^2, \\
y_3 &= (kX(2k - X) + 2\sqrt{k}Y(2k + X))^2, \\
y_4 &= (3kX(2k + X) + 2\sqrt{k}Y(2k - X))^2.
\end{align*}
\]

3. If \( \{y_1, y_2, \ldots, y_n\} \subseteq \mathbb{Q} \) are \( n \geq 4 \) squares in an arithmetic progression over \( \mathbb{Q} \), then \( (y_1:y_2: \cdot \cdot \cdot : y_n) = (1:1: \cdot \cdot \cdot : 1) \).

**Proof.** Set \( y_1 = x_1^2 \), \( y_2 = x_2^2 \), \( y_3 = x_3^2 \), and \( y_4 = x_4^2 \). For the first statement, use the transformation

\[
\begin{align*}
x_1^2 - 3x_2^2 + 3x_3^2 - x_4^2 &= 0, \\
2x_1 - 3x_2 - 3x_3 + x_4 &= X, \\
6x_1 - x_2 + x_3 - x_4 &= Y.
\end{align*}
\]

The equations \( x_1^2 - 2x_2^2 + x_3^2 = x_2^2 - 2x_3^2 + x_1^2 = 0 \) are equivalent to the one equation \( Y^2 = X^3 + 5X^2 + 4X \). For the second statement, use the fact that \((kU : \sqrt{k}V : k^2)\) is a \( K(\sqrt{k}) \)-rational point on the elliptic curve \( Y^2 = X^3 + 5X^2 + 4X \) whenever \((U : V : 1)\) is a \( K \)-rational point on the quadratic twist \( V^2 = U^3 + 5kU^2 + 4k^2U \). For the last statement, we use the rational points in Table 1: the right-hand column is the exhaustive list of all \( \mathbb{Q} \)-rational points \((X : Y : 1)\) on \( Y^2 = X^3 + 5X^2 + 4X \).

The elliptic curve \( Y^2 = X^3 + 5X^2 + 4X \) is the same as the modular curve \( X_0(24) \), where \( X_0(24)(\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_4 \) is a finite group. (We will provide a formal definition of modular curves in the next section.) The results above give a sufficient condition for there to be nonconstant four-term arithmetic progressions whose terms are perfect.
squares in $K = \mathbb{Q}(\sqrt{k})$ by considering $K$-rational points on $X_0(24)^{(k)}$. For example, when $k = 6$, the quadratic twist $Y^2 = X^3 + 5kX^2 + 4k^2X$ has a $\mathbb{Q}$-rational point $(X : Y : 1) = (-8 : -16 : 1)$, so that we find an arithmetic progression of four squares over $K = \mathbb{Q}(\sqrt{6})$: 

$$(y_1 : y_2 : y_3 : y_4) = ((9 - 5\sqrt{6})^2 : (15 - \sqrt{6})^2 : (15 + \sqrt{6})^2 : (9 + 5\sqrt{6})^2).$$

However, not all arithmetic progressions of four squares over $K = \mathbb{Q}(\sqrt{k})$ are in this form. In 2009, González-Jiménez and Xarles [6] found the following arithmetic progression of five squares over $K = \mathbb{Q}(\sqrt{409})$: 


3. Arithmetic Progressions on Conic Sections

The set $\{1, 25, 49\}$ is a 3-term collection of integers which forms an arithmetic progression. We view the set $\{(1 : 1 : 1), (5 : 25 : 1), (7 : 49 : 1)\}$ as a 3-term collection of rational points $(x : y : 1)$ on the parabola $y = x^2$ whose $y$-coordinates form an arithmetic progression. This motivates a natural generalization of arithmetic progressions on conics. Consider an arbitrary conic section as viewed in the projective plane:

$$C = \{(x_1 : x_2 : x_0) \in \mathbb{P}^2 | Ax_1^2 + 2Bx_1x_2 + Cx_2^2 + 2Dx_1x_0 + 2Ex_2x_0 + Fx_0^2 = 0\}.$$

Upon fixing a linear rational map $\ell$, we have a map

$$C(K) \times \mathbb{P}^1(K), \quad (x_1 : x_2 : x_0) \mapsto \frac{ax_1 + bx_2 + cx_0}{dx_1 + ex_2 + fx_0}.$$

We will call a set $\{P_1, P_2, \ldots, P_n\} \subseteq \mathbb{P}^2(K)$ an arithmetic progression on $C$ with respect to $\ell$ if

(i) each $P_i \in C(K)$ is a point on the conic section, and
(ii) there is a common difference $\delta = \ell(P_{i+1}) - \ell(P_i)$.
For *squares* in an arithmetic progression we would choose the parabola $C : y = x^2$ and the linear polynomial $\ell(x, y, 1) = y$. We are interested in the intersection of a line $\ell(x_1, x_2, x_0) = t$ with the conic $C(K)$ where we allow $t \in K$ to vary.

**Proposition 3.1.** Fix a conic section

$$C : Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0$$

and a linear rational map $\ell(x, y, 1) = (ax + by + c)/(dx + ey + f)$ over a field $K$ of characteristic different from 2. For any $t \in K$, define the discriminant via the quadratic polynomial

$$\text{Disc}(t) = \begin{vmatrix} a - dt & b - et & c - ft \\ E^2 - CF & BF - DE & CD - BE \\ BF - DE & D^2 - AF & AE - BD \\ CD - BE & AE - BD & B^2 - AC \end{vmatrix}.$$  

If there is a point $P = (x_1 : x_2 : x_0)$ in $C(K)$ satisfying $\ell(P) = t$, then $\sqrt{\text{Disc}(t)} \in K$, and the coordinates must be of the form

$$x_1(t) = B(b - et)(c - ft) - C(a - dt)(c - ft) - D(b - et)^2 + E(a - dt)(b - et) \pm (b - et)\sqrt{\text{Disc}(t)},$$

$$x_2(t) = -A(b - et)(c - ft) + B(a - dt)(c - ft) + D(a - dt)(b - et) - E(a - dt)^2 \mp (a - dt)\sqrt{\text{Disc}(t)},$$

$$x_0(t) = A(b - et)^2 - 2B(a - dt)(b - et) + C(a - dt)^2.$$  

Conversely, if $\sqrt{\text{Disc}(t)} \in K$, then $P = (x_1(t) : x_2(t) : x_0(t))$ is a point in $C(K)$ satisfying $\ell(P) = t$.

**Proof.** It is easy to verify that $x_1 = x_1(t)$, $x_2 = x_2(t)$, and $x_0 = x_0(t)$ as above is the solution to the simultaneous equations

$$(a - dt)x_1 + (b - et)x_2 + (c - ft)x_0 = 0,$$

$$Ax_1^2 + 2Bx_1x_2 + Cx_2^2 + 2Dx_1x_0 + 2Ex_2x_0 + Fx_0^2 = 0.$$  

Similarly, it is easy to verify that the $3 \times 3$ determinant

$$\begin{vmatrix} a & b & c \\ d & e & f \\ Ax_1 + Bx_2 + Dx_0 & Bx_1 + Cx_2 + Ex_0 & Dx_1 + Ex_2 + Fx_0 \\ dx_1 + cx_2 + fx_0 & dx_1 + cx_2 + fx_0 & dx_1 + cx_2 + fx_0 \end{vmatrix}$$

has the value $\pm \sqrt{\text{Disc}(t)}$, and hence must be an element of $K$.  

We explain how Proposition 3.1 is related to Proposition 2.1 and Theorem 2.3. For the parabola $C : y = x^2$ and the linear polynomial $\ell(x, y, 1) = y$, we have the
discriminant $\text{Disc}(t) = t$. The corresponding points on the parabola are $P = (\pm \sqrt{7} : t : 1)$. In order to have an arithmetic progression $\{y_1, y_2, \ldots, y_n\} \subseteq K$ of squares, we must choose $y_i = t_i = x_i^2$. The difficulty in creating an arithmetic progression is forcing $\delta = t_{i+1} - t_i$ to be a constant.

3.1. Three squares in arithmetic progression revisited

The following result gives a generalization to the infinitude of three rational squares in an arithmetic progression.

**Theorem 3.2.** Continue notation as in Proposition 3.1. Assume that there exists $t_0 \in K$ such that $\sqrt{\text{Disc}(t_0)} \in K$, and define the quantity

$$k = \frac{\text{Disc}'(t_0)^2 - 2 \text{Disc}(t_0) \text{Disc}''(t_0)}{\text{Disc}'(t_0)^2} \in K.$$  

1. There exist nontrivial sequences $\{t_1, t_2, \ldots, t_n\} \subseteq K$ such that each $\sqrt{\text{Disc}(t_i)} \in K$. In particular, each $K$-rational point $P_i = (x_1(t_i) : x_2(t_i) : x_0(t_i))$ is in $\mathcal{C}(K)$, and $\ell(P_{i+1}) - \ell(P_i) = t_{i+1} - t_i$.

2. There exists an arithmetic progression $\{P_1, P_2, P_3\} \subseteq \mathbb{P}^2(K)$ on $\mathcal{C}$ with respect to $\ell$. Moreover, the points must necessarily be of the form $P_i = (x_1(t_i) : x_2(t_i) : x_0(t_i))$ in terms of

\[
\begin{align*}
t_1 &= t_0 - \delta \\
t_2 &= t_0 \\
t_3 &= t_0 + \delta
\end{align*}
\]

for some $K$-rational point $(X : Y : 1)$ on the cubic curve

$$\mathcal{E}_k : Y^2 + 4XY + 4kY = X^3 + kX^2.$$  

**Proof.** Assume that $\sqrt{\text{Disc}(t)} \in K$ for some $t \in K$, and define the quantities

$$c_n = \frac{1}{\text{Disc}(t)^n} \frac{d^n}{dt^n} \left[ \frac{\text{Disc}(t)}{n!} \right] \Rightarrow \frac{\text{Disc}(t + \delta)}{\text{Disc}(t)} = c_0 + c_1 \delta + c_2 \delta^2.$$  

(Note that $c_0 = 1$.) Then $\sqrt{\text{Disc}(t + \delta)} \in K$ for some nonzero $\delta \in K$ if and only if the following quantity is $K$-rational:

$$u = \frac{\sqrt{\text{Disc}(t + \delta)} - \sqrt{\text{Disc}(t)}}{\delta \sqrt{\text{Disc}(t)}} \Rightarrow \delta = \frac{c_1 - 2u}{u^2 - c_2}.$$  

because $(\delta u + 1)^2 = \text{Disc}(t + \delta)/\text{Disc}(t) = c_0 + c_1 \delta + c_2 \delta^2$. Inductively, if $\sqrt{\text{Disc}(t_i)} \in K$ for some $t_i = t \in K$, then we can find $\delta \in K$ as a function of $t_i$ and $u$ such that $\sqrt{\text{Disc}(t_{i+1})} \in K$ for $t_{i+1} = t + \delta \in K$. 


If $\sqrt{\text{Disc}(t \pm \delta)}$ are simultaneously $K$-rational, then define the quantities

$$u = \frac{\sqrt{\text{Disc}(t + \delta)} - \sqrt{\text{Disc}(t)}}{\delta^{\sqrt{\text{Disc}(t)}}} \quad \text{and} \quad v = \frac{\sqrt{\text{Disc}(t - \delta)} - \sqrt{\text{Disc}(t)}}{\delta^{\sqrt{\text{Disc}(t)}}}$$

so that we have the identities

$$\left(\frac{\delta v + 1}{\delta u + 1}\right)^2 = \frac{\text{Disc}(t - \delta)}{\text{Disc}(t + \delta)} = \frac{c_0 - c_1 \delta + c_2 \delta^2}{c_0 + c_1 \delta + c_2 \delta^2} = \frac{u^4 + 2c_1 u^3 + (2c_2 - c_1^2) u^2 - 6c_1 c_2 u + c_2(c_2 + 2c_1^2)}{(u^2 - c_1 u + c_2)^2}.$$

This is a quartic curve, so we transform into a cubic curve using the ideas in Cassels [2, Chap. 8]. Using the birational transformations

$$X = 2k \left(\frac{c_1}{v - u - c_1}\right) \quad \Rightarrow \quad \left\{\begin{array}{l}
u = c_1 + Y + X, \\u = c_1 + Y + 3X + 4k, \\
2X.
\end{array}\right.$$  

it is easy to see that the quartic identity above is equivalent to the cubic relation $Y^2 + 4XY + 4k = X^3 + kX^2$ in terms of the $K$-rational quantity $k = (c_1^2 - 4c_2)/c_1^2$ as in Eq. (1.1). Conversely, if $(X : Y : 1)$ is a $K$-rational point on the cubic curve, then both $\sqrt{\text{Disc}(t \pm \delta)} \in K$ simultaneously when we choose the common difference

$$\delta = c_1 - 2u = \frac{-c_1 - 2v}{u^2 - c_2} = \frac{1}{c_1} \frac{4XY}{Y^2 + 2XY + kX^2}.$$

This completes the proof. $\square$

We explain how Theorem 3.2 is related to Proposition 2.1. For the parabola $\mathcal{C} : y = x^2$ and the linear polynomial $\ell(x, y, 1) = y$, we have the discriminant $\text{Disc}(t) = t$. We choose a nonzero square $t_0 = x_0^2$ so that $\sqrt{\text{Disc}(t_0)} = x_2 \in K$. As $k = 1$ in this case, the cubic curve $Y^2 + 4XY + 4k = X^3 + kX^2$ is singular, so that we have a rational parametrization of $K$-rational points $(X : Y : 1)$.

$$t = -\frac{Y + 3X + 4}{Y + X} \quad \Rightarrow \quad \left\{\begin{array}{l}X = \frac{-1}{4} \frac{t}{(t + 1)^2}, \\Y = \frac{1}{16} \frac{t - 1}{(t + 1)^3}.
\end{array}\right.$$

This yields the common difference

$$\delta = \frac{4XY}{c_1 Y^2 + 2XY + kX^2} = \frac{4(t^3 - t)}{(t^2 + 1)^2} x_2^2.$$
for the $K$-rational squares

\[
\begin{align*}
y_1 &= t_0 - \delta = \left( \frac{t^2 - 2t - 1}{t^2 + 1} \cdot x_2 \right)^2, \\
y_2 &= t_0 = x_2^2, \\
y_3 &= t_0 + \delta = \left( \frac{t^2 + 2t - 1}{t^2 + 1} \cdot x_2 \right)^2.
\end{align*}
\]

3.2. Relation with modular curves and moduli spaces

There is quite a bit of symmetry in the general construction above.

**Proposition 3.3.** Continue notation as in Proposition 3.1 and Theorem 3.2, and assume that

\[
E_k : Y^2 + 4XY + 4kY = X^3 + kX^2
\]

is an elliptic curve. Translation $(X : Y : 1) \mapsto (0 : 0 : 1) \oplus (X : Y : 1)$ yields a permutation $\sigma$ of order 4, while inversion $(X : Y : 1) \mapsto [-1](X : Y : 1)$ yields a permutation $\tau$ of order 2. The group

\[
D_4 \simeq \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \tau \circ \sigma \circ \tau = \sigma^{-1} \rangle
\]

acts on $E_k(K)$, and sends $\delta \mapsto \pm \delta$.

**Proof.** It is easy to verify that $(0 : 0 : 1) \in E_k(K)$ is a torsion point of order 4. It is also straightforward to verify the following maps:

\[
\sigma : \begin{cases} 
X &\mapsto -4kY/X^2 \\
Y &\mapsto 4k^2(X^2 - 4Y)/X^3 \\
u &\mapsto (c_1v + 2c_2)/(2v + c_1) \\
\delta &\mapsto -\delta
\end{cases}, \quad \tau : \begin{cases} 
X &\mapsto X \\
Y &\mapsto -Y - 4X - 4k \\
u &\mapsto -u \\
\delta &\mapsto -\delta
\end{cases}
\]

Hence $\sigma^4 = \tau^2 = 1$ while $\tau \circ \sigma \circ \tau = \sigma^{-1}$.

Proposition 3.3 hints at the many properties of $E_k$ from Theorem 3.2. This cubic curve is quite general.

**Proposition 3.4.** Let $K$ be a field of characteristic different from 2. Then any elliptic curve $E$ over $K$ with a $K$-rational point $P$ of order 4 must be isomorphic to

\[
E_k : Y^2 + 4XY + 4kY = X^3 + kX^2,
\]

where $k \neq 0, 1, \infty$ and $P_k = (0 : 0 : 1)$.
Proof. This can be found in [9, Table 3, p. 217] and Husemoller [7, Example (4.6)(a), p. 94], but we provide a relatively self-contained proof. Without loss of generality, assume that \( P = (x_0 : y_0 : 1) \) is a point of order 4 on the Weierstrass equation

\[
E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.
\]

If we define the coefficients

\[
\begin{align*}
    b_2 &= a_1^2 + 4a_2, \\
    b_4 &= a_1 a_3 + 2a_4, \\
    b_6 &= a_3^2 + 4a_6, \\
    b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2
\end{align*}
\]

and then substitute

\[
\begin{align*}
    k_1 &= \frac{2y_0 + a_1 x_0 + a_3}{6x_0^2 + b_2 x_0 + b_4}, \\
    k_2 &= 16 \frac{3x_0^4 + b_2 x_0^3 + 3b_4 x_0^2 + 3b_6 x_0 + b_8}{(6x_0^2 + b_2 x_0 + b_4)^2}, \\
    k_3 &= 16 \frac{(2y_0 + a_1 x_0 + a_3)^4}{(6x_0^2 + b_2 x_0 + b_4)^3}, \\
    X &= 16k_1^2(x - x_0), \\
    Y &= 64k_3^2(y - y_0) + 32k_1^2(a_1 k_1 - 1)(x - x_0),
\end{align*}
\]

then \( E \) has the equation \( Y^2 + 4XY + 4k_3 Y = X^3 + k_2 X^2 \) while \( P \) maps to the point \((0 : 0 : 1)\). It is easy to verify that

\[
[4](0 : 0 : 1) = 4k_2(k_3 - k_2)(16k_3^2 - 16k_3 k_2 + k_2^2)
\]

\[
: k_2^2(32k_3^2 - 48k_3 k_2 + 16k_2^2 + k_2^3) : 64(k_3 - k_2)^2
\]

and so \((0 : 0 : 1)\) has order 4 if and only if \( k_2 = k_3 \). Upon denoting \( k = k_2 = k_3 \), we see that \( E \cong E_k \) is an elliptic curve if and only if \( k \neq 0, 1, \infty \).

We offer a general discussion regarding Proposition 3.4 in order to explain the general framework. We introduce modular curves and moduli spaces. To this end, recall that the extended upper half-plane \( \mathbb{H} = \{ x + iy \mid y > 0 \} \cup \mathbb{P}^1(\mathbb{Q}) \) is isomorphic to the unit disk via the map \( \mathbb{H} \rightarrow \mathbb{P}^1(\mathbb{C}) \) which sends \( \tau \) to \( q = e^{2\pi \tau} \), and we have a left action

\[
\circ : \text{SL}_2(\mathbb{Z}) \times \mathbb{H} \rightarrow \mathbb{H} \text{ defined by } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \circ \tau = \frac{a \tau + b}{c \tau + d}.
\]
For any positive integer $N$, we consider the congruence subgroups
\[
\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\},
\]
\[
\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z}) \mid a \equiv d \equiv 1, c \equiv 0 \pmod{N} \right\}.
\]
We have a commutative diagram
\[
\begin{array}{ccc}
\mathbb{H} / \Gamma_0(4) & \overset{k}{\longrightarrow} & \mathbb{P}^1(\mathbb{C}) \\
\downarrow & & \downarrow \\
\mathbb{H} / \Gamma_1(2) & \overset{r}{\longrightarrow} & \mathbb{P}^1(\mathbb{C}) \\
\downarrow & & \downarrow \\
\mathbb{H} / \Gamma_1(1) & \overset{j}{\longrightarrow} & \mathbb{P}^1(\mathbb{C})
\end{array}
\]
where $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$ is the divisor function, the horizontal arrows are bijections, and we have the identities $j(\tau) = (r(\tau) + 256)^3 / r(\tau)^2$ and $r(\tau) = 16k(\tau)^2 / (1 - k(\tau))$ coming from the vertical arrows. These maps are defined over $\mathbb{C}$, but we wish to give an interpretation over any field $K$ of characteristic different from 2. The moduli spaces $X_0(N)$ and $X_1(N)$ consist of pairs $(E, C)$ and $(E, P)$ of elliptic curves $E$ with either a cyclic subgroup $C$ of order $N$ or a specified point $P$ of order $N$, respectively. We have $X_0(N)(\mathbb{C}) \simeq \mathbb{H} / \Gamma_0(N)$ and $X_1(N)(\mathbb{C}) \simeq \mathbb{H} / \Gamma_1(N)$, but we are interested in $K$-rational points. By “forgetting” the level structures, we have a commutative diagram
\[
\begin{array}{ccc}
\mathbb{P}^1(K) & \overset{E_k}{\longrightarrow} & X_1(4)(K) \\
\downarrow & & \downarrow \\
\mathbb{P}^1(K) & \overset{E_r}{\longrightarrow} & X_1(2)(K) \\
\downarrow & & \downarrow \\
\mathbb{P}^1(K) & \overset{E_j}{\longrightarrow} & X_1(1)(K)
\end{array}
\]
where $E_k : Y^2 + 4XY + 4kY = X^3 + kX^2$, $P_k = (0 : 0 : 1)$, $E_r : Y^2 = X^3 + 2X^2 + r/(r + 64)X$, $Q_r = (0 : 0 : 1)$, and $E_j : Y^2 + XY = X^3 + 36/(1728 - j)X + 1/(1728 - j)$, $O_j = (0 : 1 : 0)$.
where the horizontal arrows sending $k \mapsto (E_k, P_k)$ and $j \mapsto (E_j, O_j)$ are bijections as in Proposition 3.4, and we have the two relations $j = (r + 256)^3/r^2$ and $r = 16k^2/(1 - k)$ coming from the vertical arrows. (Not every $X_0(N)$ or $X_1(N)$ is birationally equivalent to $\mathbb{P}^1$: as mentioned in the previous section, $X_0(24)$ is the elliptic curve $Y^2 = X^3 + 5X^2 + 4X$.)

### 3.3. Congruent numbers revisited

Theorem 3.2 gives an explicit way to write down arithmetic progressions $\{P_1, P_2, P_3\} \subseteq \mathbb{P}^2(K)$ on a conic section

$$C = \{(x_1 : x_2 : x_0) \in \mathbb{P}^2 | Ax_1^2 + 2Bx_1x_2 + Cx_2^2 + 2Dx_1x_0 + 2Ex_2x_0 + Fx_0^2 = 0\}$$

with respect to a linear rational map

$$C(K) \to \mathbb{P}^1(K), \quad (x_1 : x_2 : x_0) \mapsto \frac{ax_1 + bx_2 + cx_0}{dx_1 + ex_2 + fx_0}$$

defined over a field $K$ of characteristic different from 2. Consider those $t_0 \in K$ such that $\sqrt{\text{Disc}(t_0)} \in K$ and $k \neq 0, 1, \infty$ as in Eq. (1.1), Eq. (1.2), and Proposition 3.1. For each $K$-rational point $(X : Y : 1)$ on the elliptic curve

$$E_k : Y^2 + 4XY + 4kY = X^3 + kX^2$$

the desired set is

$$\{P_1, P_2, P_3\} = \left\{(x_1(t_0 - \delta) : x_2(t_0 - \delta) : x_0(t_0 - \delta)), (x_1(t_0) : x_2(t_0) : x_0(t_0)), (x_1(t_0 + \delta) : x_2(t_0 + \delta) : x_0(t_0 + \delta))\right\}$$

as in Eq. (1.3). We have seen that the dihedral group $D_4$ of order 8 coming from translation by 4-torsion on $E_k$ acts on the points $(X : Y : 1) \in E_k(K)$ and sends $\delta \mapsto \pm \delta$. We generalize Corollary 2.2 by asking which common differences of arithmetic progressions on conic sections with respect to linear rational maps.

**Corollary 3.5.** For each nonzero $\delta \in K$, denote the quantities

- $A = \text{Disc}(t) - \text{Disc}(t - \delta) = \text{Disc}'(t)\delta - \text{Disc}''(t)\delta^2/2$,
- $B = \text{Disc}(t + \delta) - \text{Disc}(t) = \text{Disc}'(t)\delta + \text{Disc}''(t)\delta^2/2$,
- $C = \text{Disc}(t + \delta) - \text{Disc}(t - \delta) = 2\text{Disc}'(t)\delta$.

Then the following statements are equivalent.

1. There exist $x_1, x_2, x_3 \in K$ such that $x_2^2 - A = x_1^2$ and $x_2^2 + B = x_3^2$.
2. There exist $X, Y \in K$ with $Y \neq 0$ such that $Y^2 = X(X - A)(X + B)$.
3. Upon defining an “angle” $\theta$ by $\cos \theta = (B - A)/C$, there exist $a, b, c \in K$ such that $a^2 - 2ab\cos \theta + b^2 = c^2$ and $(1/2)ab\sin \theta = \sqrt{AB}$.
We remind the reader that $K$ is any field of characteristic different from 2, so the “angle” $\theta$ may not be defined in the usual sense. We only consider the symbols $\cos \theta$ and $\sin \theta$ as formal elements from an algebraic closure of $K$ such that $(\cos \theta)^2 + (\sin \theta)^2 = 1$.

**Proof of Corollary 3.5.** Following the proof of Theorem 3.2, the quantities $A$ and $B$ are chosen so that we have the identities

$$
\begin{align*}
x_1 &= \sqrt{\text{Disc}(t - \delta)} \\
x_2 &= \sqrt{\text{Disc}(t)} \\
x_3 &= \sqrt{\text{Disc}(t + \delta)}
\end{align*}
$$

This motivates the following transformations:

$$
\begin{align*}
X &= \frac{AB(x_1 - x_3)}{Bx_1 - Cx_2 + Ax_3} \\
Y &= \frac{ABC}{Bx_1 - Cx_2 + Ax_3}
\end{align*}
$$

Hence $A = x_2^2 - x_1^2$ and $B = x_3^2 - x_2^2$ if and only if $Y^2 = X(X - A)(X + B)$ for some nonzero $Y$. Similarly, we have the following transformation:

$$
\begin{align*}
a &= \frac{X^2 + (B - A)X - AB}{Y} \\
b &= \frac{CX}{Y} \\
c &= \frac{X^2 + AB}{Y}
\end{align*}
$$

Hence $Y^2 = X(X - A)(X + B)$ for some nonzero $Y$ if and only if $a^2 - 2ab \cos \theta + b^2 = c^2$ and $ab \sin \theta = 2\sqrt{AB}$.

We explain how Corollary 3.5 is related to Corollary 2.2. For the parabola $C : y = x^2$ and the linear polynomial $\ell(x, y, 1) = y$, we have the discriminant $\text{Disc}(t) = t$. Then $A = B = \delta$ and $C = 2\delta$ in this case, so that we have the elliptic curve $Y^2 = X^3 - \delta^2 X$.

In general, common differences $\delta$ for a 3-term arithmetic progression $\{P_1, P_2, P_3\}$ on a conic section $C$ with respect to a linear rational map $\ell$ correspond to nontrivial rational points $(X : Y : 1)$ on the Frey curve $Y^2 = X(X - A)(X + B)$. Geometrically, we can construct a $K$-rational triangle having rational sides of length $a, b, c$ and having a common angle $\theta$ such that the area is $\sqrt{AB}$. This is very similar to the concept of a $\theta$-congruent number as defined by Fujisawa [4]. We have decided not to use this language in the exposition at hand because the area $\sqrt{AB}$ is not always a linear function of the difference $\delta$. 


Acknowledgment

We would like to thank the referee for a careful reading of this manuscript.

References


