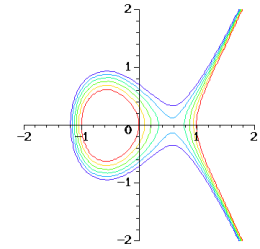


Arithmetic Progressions on Elliptic Curves

Alejandra Alvarado

under the supervision of Dr. Andrew Bremner



ABSTRACT Consider an elliptic curve of the form, $y^2 = f(x)$, over the rationals. We investigate arithmetic progressions in the x and y coordinates on a special type of elliptic curve.

Definition 1. An arithmetic progression (AP) is a sequence of numbers such that the difference between any two consecutive numbers is constant. When we talk about an arithmetic progression on a curve $y^2 = f(x)$, we mean an arithmetic progression in the x or y coordinates.

Note: Most of the calculations were done using several computer algebra software programs.

Consider curves of the form $y^2 = f(x)$ over \mathbb{Q} , where $f(x)$ is a degree 3 polynomial. Bremner [3] and Campbell [6] have found distinct infinite families of elliptic curves, with x coordinate APs of length 8. They also found a curve with y -AP of length 7.

An interesting article by Garcia-Saeta and Tomero [9], considers simultaneous APs on these curves, of lengths 3, 4 and 5. The authors found at least 2 examples of simultaneous AP of length 5. They also found a curve with y -AP of length 7.

In a more recent article [10], the authors found examples and proved that only finitely many non-isomorphic curves exist with simultaneous AP of length 6. They also proved that no elliptic curves exist with simultaneous AP of length 7.

Integral Arithmetic Progressions on $y^2 = x^3 + k$

Consider the curve

$$E: y^2 = x^3 + k$$

where $k \neq 0$ is an integer and E is defined over \mathbb{Q} . We investigate arithmetic progressions on these curves, of lengths 3, 4 and 5. Mohanty [14] showed that no x -APs exist of length 3 or more with difference 1.

In Lee & Velaz [12], the authors found infinitely many sets of solutions with x -AP length 4. They also construct infinitely many solutions with y -AP of length 4, 5 and 6.

Length 3 y -AP

$$\begin{aligned} (a-d)^2 &= p^3 + k & \Rightarrow & 4ad = p^3 - p^3 \\ a^2 &= q^3 + k & \Rightarrow & 2d^2 = p^3 - 2q^3 + p^3 \\ (a+d)^2 &= r^3 + k \end{aligned}$$

If we write $(p, q, r, d) = (F, G, H, D)$, for some parameter t , then:

$$\begin{aligned} F &= 2(t^3 - 2Q^2 + R^2) \\ D &= (t^3 - 2Q^2 + R^2) \\ G &= (t^3 - 2Q^2 + R^2)(t^3 - p^3) \\ H &= (t^3 - 2Q^2 + R^2)(t^3 - 2R^2t^3 - 8Q^2t^3 + 16Q^6 - 8Q^2t^3 + R^6) \end{aligned}$$

We thus have a infinitely many curves with length 3 y -AP.

Length 4 y -AP

$$\begin{aligned} (a-3d)^2 &= p^3 + k \\ (a-d)^2 &= q^3 + k \\ (a+d)^2 &= r^3 + k \\ (a+3d)^2 &= s^3 + k \end{aligned}$$

We will then consider the problem of finding rational points on the cubic surface in \mathbb{P}^3 :

$$S: y^3 - 3y^2 + 3y - x^3 = 0$$

On our surface S , we know a pair of skew lines which are conjugate over \mathbb{C} .

$L_1: y - ux = q - u = 0, L_2: y - u^2x = q - u^2 = 0$ where $u^3 = 1$. Let $P_1 \in L_1$ and $P_2 \in L_2$ where P_1 is conjugate to P_2 .

$$P_1 = (u_1, v_1, r_1, s_1) = (u - u^2, u^2, 1, u^2 - u)$$

$P_2 = (u_2, v_2, r_2, s_2) = (u - u^2, u^2, 1, u^2 - u)$, where (u, v) are rational parameters. The line joining P_1 to P_2 is:

$L = \{(1u_1 + \mu u_2, \nu_1 + \mu \nu_2, \rho_1 + \mu \rho_2, \sigma_1 + \mu \sigma_2) : \lambda \neq 0 \text{ or } \mu \neq 0\}$. This line intersects the surface in one other point. In order to find this point, substitute a general point on the line, into the equation for S . The third point lies on the surface when:

$$\begin{aligned} \lambda &= 18 + 3u^3 - 3u^6 + 9u^2 + 9u^2 + 6u^3 + 9u^2 + 3u^6 + 9u \\ \mu &= -(6u^3 + 3u^6 + 9u^2 + 9u^2 + 9u^2 - 3u^6 + 3u^6 - 9u + 9) \end{aligned}$$

Substituting these values for (λ, μ) gives us a rational point which lies on the line and the surface, namely, the third point of intersection:

$$\begin{aligned} p &= u^4 + 2u^3 + 3u^2 + 2u^2 - 3u + u^4 + 3u \\ q &= -(2u^3 + 3u^2 + 3u^2 + u^3 + 3) \\ r &= u^3 - u^3 + 3 \\ s &= u^4 + 2u^3 + 3u^2 + 2u^2 + 6u + u^4 + 3u \end{aligned}$$

Length 5 y -AP on $y^2 = x^3 + k$

Consider y -AP of the form $\{-2d, d, 0, d, 2d\}$.

$$\begin{aligned} 0 &= p^3 + k \\ d^2 &= q^3 + k \\ 4d^2 &= r^3 + k \end{aligned}$$

We will then consider the problem of finding rational points on the elliptic curve in \mathbb{P}^2 :

$$C: y^3 - 4y^2 + 3y^3 = 0$$

whose rank 1 minimal model is

$$E: y^2 = x^3 - 97x$$

Thus, points on the free part of E map to points on C which give us a length 5 y -AP.

Now suppose our y -AP is of the form $\{4, 2d, 3d, 4d, 5d\}$.

$$\begin{aligned} d^2 &= p^3 + k & -9p^3 + 8p^3 - 3p^3 = 0 \\ 4d^2 &= q^3 + k & -4q^3 + 5q^3 - p^3 = 0 \\ 9d^2 &= r^3 + k & -7r^3 + 6r^3 - p^3 = 0 \\ 16d^2 &= s^3 + k & \\ 25d^2 &= t^3 + k & \end{aligned}$$

The last 3 equations represent 3 curves in \mathbb{P}^2 . By the Riemann-Hurwitz formula, this curve has genus 55. This implies there are only finitely many points on the curve. Thus, there are only finitely many (possibly none) curves with length 5 y -AP.

Length 3 x -AP

$$\begin{aligned} (r-a)^2 + k &= p^2 \\ a^2 + k &= q^2 \\ (a+r)^2 + k &= r^2 \end{aligned}$$

After some rewriting, we have

$$12a^2 + 6a^2(p^2 - r^2) + (p^2 + r^2 - 2a^2)^2 = 0.$$

The quadratic yields

$$12a^3 = -3(p^2 - r^2) \pm \sqrt{9(p^2 - r^2)^2 - 12(p^2 + r^2 - 2a^2)^2}$$

We require the expression inside the radical to be a square:

$$9(p^2 - r^2)^2 - 12(p^2 + r^2 - 2a^2)^2 = 0.$$

Let $\alpha = (p^2 - r^2)/(p^2 + r^2)$. Substitute back,

$$\alpha^2 - 16\alpha + 16 = -3\alpha^2 \quad (1)$$

for some rational δ . Notice (2,2) is a point on the conic (1). We can then parametrize all rational solutions by substituting $\delta = (\alpha - 2) + 2\alpha(1, t)$. For rational t , to reveal $(\alpha, \delta) = (2, 2)$ or $(\alpha, \delta) = \left(\frac{2(2t^2 - 6t + 1)}{3t^2 + 1}, \frac{-2(2t^2 - 6t + 1)}{3t^2 + 1}\right)$.

Substituting for α , we want to parametrize the curve over \mathbb{Q} :

$$C: (p^2 - r^2)(3p^2 + 1) = 2(p^2 - r^2)(3p^2 - 6t + 7).$$

Notice $(p, r) = (1, 1)$ is a point on the curve, so we can parametrize the ratio $(p : r)$ in terms of (u, v) .

$$\begin{aligned} p &= (-3u^2 - 1)v^2 + (-12v^2 - 2u - 20)u + (-6v^2 + 12v - 14)u^2 \\ q &= (-3u^2 - 1)v^2 + (-6v^2 - 2)u + (-6v^2 + 12v - 14)u^2 \\ r &= (-3u^2 - 1)v^2 + (6v^2 + 12v + 14)u^2 \end{aligned}$$

From here, we can find parametrizations of (x, k) in terms of (u, v) .

Length 4 x -AP

$$\begin{aligned} (a-3d)^2 + k &= p^2 \\ (a-d)^2 + k &= q^2 \\ (a+d)^2 + k &= r^2 \\ (a+3d)^2 + k &= s^2 \end{aligned}$$

We will then consider the problem of finding rational points on the cubic surface in \mathbb{P}^3 :

$$S: (p^2 - 21d^2 + 27d^2 - 2^2)(-p^2 + 3d^2 - 2a^2 + r^2) = 3(p^2 - q^2 - r^2 + s^2)^2$$

The singular points on the surface are:

- (1, 1, 1, 1)
- (1, 1, -1, 1)
- (1, -1, 1, -1)
- (1, -1, -1, -1)
- (1, 1, 1, -1)
- (1, -1, -1, 1)
- (1, 1, -1, -1)
- (1, -1, 1, 1)

Each of the following planes contain 3 of the above singularities:

- $p+q=r+s$
- $p-q=r-s$
- $p+q=r+s$
- $p-q=r-s$
- $p+q=r+s$
- $p-q=r-s$

Consider, for example, the intersection of plane (1) with S . Substitute $p = r + s - q$, we have quartic curve in \mathbb{P}^2 . Since this curve contains 3 singularities, (1),(6) and (7), by the genus formula, it is a curve of genus 0.

$$0 = 6u^2v^4 + 24u^2v^3 + 14u^2v^2 + 36v^2v^2 - 4v^2v^2 - 4v^2v^2 - 13v^4 - 20v^4 - 3v^4 - 16v^4 + 15v^4 - 6v^4 - 14v^4 + 6v^4 - 14v^4$$

which can be parametrized as follows.

- (1, 1, 1, 1)
- (1, 1, -1, 1)
- (1, -1, 1, -1)
- (1, -1, -1, -1)
- (1, 1, 1, -1)
- (1, -1, -1, 1)
- (1, 1, -1, -1)
- (1, -1, 1, 1)

$$C(x, y, z) = 40x^2 - 28z^2 - 3y^2 - 13x^2.$$

with torsion subgroup $\mathbb{Z}/2 + \mathbb{Z}/4 + \mathbb{Z}/4$. Since

$$C(\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/4$$

we have found at most 8 elliptic curves $y^2 = x^3 + k$ with integral AP $\{-2a, 0, a, 2a\}$. The identity on E does not map to a rational value of $x^2 = k$. The remaining points on E force at least two of $\{p^2, q^2, r^2, s^2\}$ to be equal, contradicting the assumption $a \neq 0$. Thus, no elliptic curves of the form $y^2 = x^3 + k$ exist with integral AP of the given form.

Special Length 5 x -AP

Consider a specific AP of the form $\{-2a, a, 0, a, 2a\}$.

$$\begin{aligned} -6a^2 + k &= p^2 & \Rightarrow & 7p^2 + 9p^2 = 16a^2 \\ -a^2 + k &= q^2 & \Rightarrow & 9p^2 + 9p^2 = 16a^2 \\ k &= r^2 & \Rightarrow & p^2 + 2a^2 = 2a^2 \\ k &= s^2 & \Rightarrow & \\ 6a^2 + k &= t^2 & \Rightarrow & \end{aligned}$$

By the Hurwitz-Riemann formula [8], the last 3 quadratic equations in \mathbb{P}^2 define a curve C of genus 5. C has maps to 5 elliptic curves. In particular, C maps to the elliptic curve defined by

$$E: y^2 = x^3 - 164x$$

which has rank zero. E 's minimal model is

$$E: y^2 = x^3 + x^2 - 164x - 964$$

The above is the equation of a conic, which can be parametrized:

$$\begin{aligned} x &= 2t^2 + 4z \\ y &= 12t \\ z &= t^2 + 39 \end{aligned}$$

This in turn leads to a parametrization of the ratio $(p : q : r : s)$:

$$\begin{aligned} p &= t^4 + 16t^2 + 60t^2 + 486t + 819 \\ q &= t^4 + 6t^2 + 60t^2 + 18t + 819 \\ r &= t^4 - 6t^2 + 60t^2 - 18t + 819 \\ s &= t^4 - 16t^2 + 60t^2 - 486t + 819 \end{aligned}$$

So for each curve on the surface that is cut out by the above planes, we can find a parametrization. If we instead write $(p, q, r, s) = (AP, AQ, AR, AS)$, we can solve for (a, d, k) in terms of t .