Arithmetic Progressions on Algebraic Curves

Szabolcs Tengely

tengely@science.unideb.hu
http://www.math.unideb.hu/~tengely

Number Theory and Cryptography Days
Selye University
Komárno

This research was supported by the European Union and the State of Hungary, co-financed by the European Social Fund in the framework of TÁMOP 4.2.4. A/2-11-1-2012-0001 'National Excellence Program'.

Summary of the talk

APs on curves

An arithmetic progression on a curve

$$F(x,y)=0,$$

is an arithmetic progression in either the x or y coordinates. One can pose the following natural question. What is the longest arithmetic progression in the x coordinates? In case of linear polynomials, Fermat claimed and Euler proved that four distinct squares cannot form an arithmetic progression.

Genus 0 curves

Allison found an infinite family of quadratics containing an integral arithmetic progression of length eight. The curve is

$$y^2 = \frac{1}{2}(k^2 - l^2)x^2 - \frac{5}{2}(k^2 - l^2)x + (3k^2 - 2l^2),$$

and the AP is as follows

$$(-1, 6k^2 - 5l^2), (0, 3k^2 - 2l^2), (1, k^2), (2, l^2), (3, l^2), (4, k^2), (5, 3k^2 - 2l^2), (6, 6k^2 - 5l^2).$$

Genus 0 curves

Arithmetic progressions on Pellian equations $x^2 - dy^2 = m$ have been considered by many mathematicians. Dujella, Pethő and Tadić proved that for any four-term arithmetic progression, except $\{0, 1, 2, 3\}$ and $\{-3, -2, -1, 0\}$, there exist infinitely many pairs (d, m) such that the terms of the given progression are y-components of solutions. Pethő and Ziegler dealt with 5-term progressions on Pellian equations.

Genus 0 curves

Aguirre, Dujella and Peral constructed 6-term AP on Pellian equations parametrized by points on elliptic curve having positive rank.
Pethő and Ziegler posed several open problems. One of them is as follows: "Can one prove or disprove that there are d and m with $d > 0$ and not a perfect square such that $y = 1, 3, 5, 7, 9$ are in arithmetic progression on the curve $x^2 - dy^2 = m$?"

Genus 0 curves

Recenlty, González-Jiménez answered the question: there is not m and d not a perfect square such that $y = 1, 3, 5, 7, 9$ are in arithmetic progression on the curve $x^2 - dy^2 = m$. He constructed the related diagonal genus 5 curve and he applied covering techniques and the so-called elliptic Chabauty's method.

Genus 1 Weierstrass curves

$$y^2 = x^3 + Ax + B$$

Bremner provided an infinite family of elliptic curve of Weierstrass form with 8 points in arithmetic progression. González-Jiménez showed that these APs cannot be extended to 9 points APs. Bremner, Silverman and Tzanakis dealt with the congruent number curve $y^2 = x^3 - n^2x$, they considered integral arithmetic progressions.

Genus 1 general cubic curves

$$y^2 = F(x)$$

If F is a cubic polynomial, then the problem is to determine arithmetic progressions on elliptic curves. Bremner and Campbell found distinct infinite families of elliptic curves, with arithmetic progression of length eight.

Genus 1 quartic curves

Campbell produced infinite families of quartic curves containing an arithmetic progression of length 9. Ulas constructed an infinite family of quartics containing a progression of length 12. Restricting to quartics possessing central symmetry MacLeod discovered four examples of length 14 progressions (e.g. $y^2 = -17x^4 + 3130x^2 + 8551, x = -13, -11, \ldots, 13.$) Alvarado extended MacLeod's list by determining 11 more examples of length 14 progressions (e.g. $y^2 = 627x^4 - 87870x^2 + 3312859$)

Genus 1 Edwards curves

$$E_d : \quad x^2 + y^2 = 1 + dx^2y^2.$$

Moody proved that there are infinitely many Edwards curves with 9 points in arithmetic progression. Bremner and independently González-Jiménez proved using elliptic Chabauty's method that Moody's examples cannot be extended to longer APs.

Genus 1 Huff curves

$$H_{a,b}: \quad x(ay^2-1)=y(bx^2-1).$$

Moody produced six infinite families of Huff curves having the property that each has rational points with x-coordinate $x=-4,-3,\ldots,3,4$. That is he obtained APs of length 9.

Summary and genus 2 cases

$m(d)$: the largest integer k such that there is a polynomial g_d of degree d with the curve $y^2 = g_d(x)$ possessing an AP of length k;
$M(d)$: the largest k such that there is an infinite family of polynomials of degree d with each member possessing an AP of length k.

d	1	2	3	4	5	6
$m(d)$	3	≥ 8	≥ 8	≥ 14	≥ 12	≥ 18
$M(d)$	3	≥ 8	≥ 8	≥ 12	≥ 12	≥ 16

Ulas: $m(5) \geq 12, M(5) \geq 11, m(6) \geq 18, M(6) \geq 16$
Alvarado: $M(5) \geq 12$.

A Diophantine problem

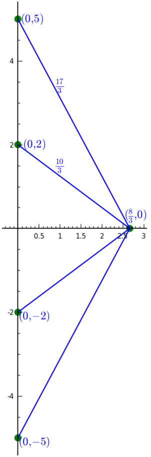
Rational distance sets

Given $a, b \in \mathbb{Q}^*$ such that $a^2 \neq b^2$. Determine the set of points $(x, 0) \in \mathbb{Q}^2$ satisfying that

$$d((0, \pm a), (x, 0)) \text{ and } d((0, \pm b), (x, 0))$$

are rational numbers.

A Diophantine problem



If $a = 2, b = 5$, then $(\frac{8}{3}, 0)$ is fine, since the two distances are $\frac{10}{3}$ and $\frac{17}{3}$.

Huff curves

Rational points on curves

Consider the Huff curve

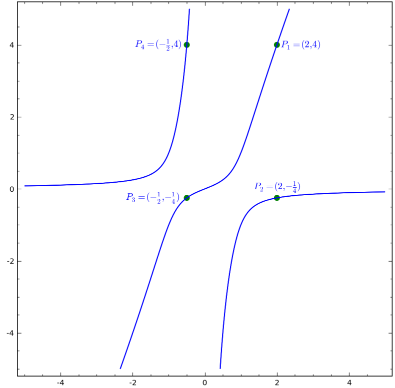
$$ax(y^2 - 1) = by(x^2 - 1).$$

If there is a rational point (x, y) on the curve, then the point

$$P = \left(\frac{2by}{y^2 - 1}, 0\right)$$

is in the distance set.

Huff curves



$(2, 4)$ is on the curve $2x(y^2 - 1) = 5y(x^2 - 1)$, hence

$$\left(\frac{2 \cdot 5 \cdot 4}{4^2 - 1}, 0\right) = \left(\frac{8}{3}, 0\right)$$

is in the distance set.

Generalized Huff curves

Wu and Feng considered the curve

$$H_{a,b}: \quad x(ay^2-1)=y(bx^2-1).$$

Moody constructed rational arithmetic progressions of length 9:

$$x \in \{-4,-3,\ldots,3,4\}.$$

Integral arithmetic progressions

We look for integral arithmetic progressions: $x_1, x_2, x_3, \ldots$ such that $(x_i, y_i) \in \mathbb{Z}^2$ are points on the curve. We have that

$$byx^2 - (ay^2 - 1)x - y = 0.$$

Therefore $F(y) = a^2y^4 + (4b - 2a)y^2 + 1 = t^2$ for some $t \in \mathbb{Z}$.

Runge's method

We define

$$P_1(y) = ay^2 - \frac{a-2b+1}{a},$$
$$P_2(y) = ay^2 - \frac{a-2b-1}{a}.$$

We obtain that

$$F(y) - P_1(y)^2 = -2\,y^2 + \frac{4\,b}{a} - \frac{4\,b^2}{a^2} + \frac{2}{a} - \frac{4\,b}{a^2} - \frac{1}{a^2},$$
$$F(y) - P_2(y)^2 = 2\,y^2 + \frac{4\,b}{a} - \frac{4\,b^2}{a^2} - \frac{2}{a} + \frac{4\,b}{a^2} - \frac{1}{a^2}.$$

Runge's method

It follows that $P_2(y)^2 < F(y) = t^2 < P_1(y)^2$ if $|y|$ is "large". That is

$$(a^2y^2 - (a-2b-1))^2 < (at)^2 < (a^2y^2 - (a-2b+1))^2.$$

Hence $t = ay^2 - \frac{a-2b}{a}$. From the equation $F(y) = t^2$ we obtain that $\frac{a-2b}{a} = \pm 1$. Thus $b = 0$ or $a = b$. If $b = 0$, then $y \in \{-1, 0, 1\}$. If $a = b$, then $x = y$ or $axy = -1$.

Runge's method

If y is not "large": we may assume that $|b| < |a|$. We have

$$\begin{aligned} F(y) - P_1(y)^2 &= -2y^2 + \frac{4b}{a} - \frac{4b^2}{a^2} + \frac{2}{a} - \frac{4b}{a^2} - \frac{1}{a^2}, \\ F(y) - P_2(y)^2 &= 2y^2 + \frac{4b}{a} - \frac{4b^2}{a^2} - \frac{2}{a} + \frac{4b}{a^2} - \frac{1}{a^2}. \end{aligned}$$

Thus

$$y \in \{-2, -1, 0, 1, 2\} \text{ and } x \in \{-2, -1, 0, 1, 2\}.$$

Hessian curves

Genus 1 curve

Hessian form of an elliptic curve:

$$x^3 + y^3 + 1 = dxy.$$

Recently, Edwards curves, Hessian curves and Huff curves turned out to have applications in elliptic curve cryptography.

Runge's method

We have that $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$, hence Runge's condition is satisfied. Let $F(x, y) = x^3 + y^3 - dxy + 1$ and

$$\begin{aligned} x &= \frac{1}{t}, \\ y &= \frac{s}{t}. \end{aligned}$$

We obtain that $F(\frac{1}{t}, \frac{s}{t}) = \frac{1}{t^3}(1 + s^3 - dst + t^3)$.

Runge's method

We apply Hensel lifting:

$$1 + s^3 - dst + t^3 = \left((s+1) + a_1 t + a_2 t^2 + \ldots\right) \times$$
$$\left((s^2 - s + 1) + (b_1 s + c_1)t + (b_2 s + c_2)t^2 + \ldots\right).$$

That is

$$g_1 = s + 1 + \frac{d}{3}t + \left(\frac{1}{3} - \frac{1}{81}d^3\right) t^3 + O(t^4),$$
$$g_2 = s^2 - s + 1 + \left(-\frac{1}{3}d - \frac{1}{3}ds\right) t + \frac{1}{9}d^2t^2 + \left(\frac{2}{3} - \frac{2}{81}d^3 - (\frac{1}{3} - \frac{1}{81}d^3)s\right) t^3 + O(t^4).$$

Runge's method

We determine a polynomial that vanishes on the branches given by g_1. Let $P(x,y) = A_0 + B_0 x + (A_1 + B_1 x)y + (A_2 + B_2 x)y^2$. We get the following system of equations:

$$\begin{aligned} \frac{1}{3}A_2 d - A_1 + B_0 &= 0, \\ \frac{1}{9}A_2 d^2 - \frac{1}{3}A_1 d + A_0 &= 0, \\ \frac{1}{81}A_2 d^3 + \frac{1}{3}A_2 &= 0. \end{aligned}$$

That is $P_1(x,y) = 3x + 3y + d$.

Runge's method

We also determine a polynomial that vanishes on the branches given by g_2. Here we obtain that

$$P_2(x, y) = 9(x^2 - xy + y^2) - 3d(x + y) + d^2.$$

We have that $P_i(x, y) \to 0$ as we move to infinity along one of the branches, that is $P_i(x, y) = 0$ if y is "large".

Runge's method

Compute when y is "large" enough:

$$
\begin{aligned}
Res_y(F, P_1 - 1) &= -27x^2 + (-9d + 9)x + d^3 - 3d^2 + 3d - 28, \\
Res_y(F, P_1 + 1) &= 27x^2 + (9d + 9)x + d^3 + 3d^2 + 3d - 26, \\
Res_y(F, P_2 - 1) &= 27x^2 + (-9d^3 + 9d + 243)x + \ldots, \\
Res_y(F, P_2 + 1) &= 27x^2 + (9d^3 + 9d - 243)x + \ldots.
\end{aligned}
$$

We get a bound (if $x \geq 4$):

$$-\frac{1}{6}d + \frac{1}{6} - h(d) \leq x \leq -\frac{1}{6}d + \frac{1}{6} + h(d),$$

where $h(d) = \frac{1}{18}\sqrt{12d^3 - 27d^2 + 18d - 327}$.

AP of length 5

We wrote a Sage code to find arithmetic progressions on Hessian curves. If $-1000 \leq d \leq 1000$, then there is a d such that a progression of length 5 exists. It is $d = -25$, on the curve $x^3 + y^3 + 25xy + 1$ there are 12 integral points. The points corresponding to the APs:

$$(-19, 27), (-13, -9), (-7, -2), P_{(-1)}, (5, -1),$$

where

$$P_{(-1)} \in \{(-1, -5), (-1, 0), (-1, 5)\}.$$

APs containing 5

Let $(x_1, y_1), (x_2, y_2), \ldots \in H(\mathbb{Z})$ points on the Hessian curve

$$H: \quad x^3 + y^3 - dxy + 1,$$

such that $x_1, x_2, \ldots$ form an AP. Assume that $x_i = 5$ for some i. We have that $d \in \{-25, 3, 19, 41, 87, 3175\}$.

Nemzeti Kiválóság Program

APs containing 5

d	APs
-25	length 5: $(-19, 27), (-13, -9), (-7, -2), (-1, -5), (5, -1)$
3	singular curve, infinite AP: $(x, -1-x)$
19	length 2, trivial APs
41	length 4: $(-1, 0), (4, -13), (9, 2), (14, 5)$, length 3: $(-1, 0), (2, 9), (5, 14)$
87	length 2, trivial APs
3175	length 2, trivial APs

If $d \neq 3$, then the longest AP containg 5 has length 5.