Powers in arithmetic progressions

Alfréd Rényi Institute of Mathematics
Number Theory Seminar

Szabolcs Tengely

15.10.2019.

University of Debrecen

Outline of talk

Powers in arithmetic progressions

$$an_i + b = x_i^\ell \text{ for } i = 1, 2, \ldots, N,$$

joint work with Lajos Hajdu.

Binomial near collisions

$$\binom{n}{k} = \binom{m}{l} + d,$$

joint work with Gallegos-Ruiz, Katsipis and Ulas.

Consecutive terms - squares

Consider consecutive terms in arithmetic progressions:

$$b = x_0^2, \quad b + a = x_1^2, \quad b + 2a = x_2^2 \quad \to \quad x_0^2 + x_2^2 = 2x_1^2.$$

Consecutive terms - squares

Consider consecutive terms in arithmetic progressions:

$$b = x_0^2, \quad b + a = x_1^2, \quad b + 2a = x_2^2 \quad \rightarrow \quad x_0^2 + x_2^2 = 2x_1^2.$$

Infinitely many solutions:

$$x_0 = p^2 - 2q^2, \quad x_1 = p^2 - 2pq + 2q^2, \quad x_2 = -p^2 + 4pq - 2q^2.$$

Consecutive terms - squares

Consider consecutive terms in arithmetic progressions:

$$b = x_0^2, \quad b + a = x_1^2, \quad b + 2a = x_2^2 \quad \to \quad x_0^2 + x_2^2 = 2x_1^2.$$

Infinitely many solutions:

$$x_0 = p^2 - 2q^2, \quad x_1 = p^2 - 2pq + 2q^2, \quad x_2 = -p^2 + 4pq - 2q^2.$$

Fermat claimed and Euler proved that that four distinct squares cannot form an arithmetic progression.

$$b(b+a)(b+2a)(b+3a) = c^2 \quad \to \quad E : y^2 = x^3 + 11x^2 + 36x + 36$$

Consecutive terms - higher powers

Darmon and Merel (1997): apart from trivial cases, there do not exist three-term arithmetic progressions consisting of n-th powers, provided $n \geq 3$.

Let

$$x_1^{l_1}, \ldots, x_t^{l_t}$$

be a primitive arithmetic progression in $\mathbb{Z}$ with $2 \leq l_i \leq L$ $(i = 1, \ldots, t)$.

Hajdu (2004): t is bounded by some constant $c(L)$ depending only on L.

Consecutive terms - higher powers

Bruin, Győry, Hajdu and Tengely (2006): proved that for any $t \geq 4$ and $L \geq 3$ there are only finitely many primitive arithmetic progressions.

Hajdu and Tengely (2009): considered the cases when the set of exponents is given by $\{2, n\}, \{2, 5\}$ and $\{3, n\}$, and (excluding the trivial cases) they showed that the length of the progression is at most six, four and four, respectively.

Consecutive terms - higher powers

Lemma (Hajdu-Tengely)

Let $\alpha = \sqrt[5]{2}$ *and put* $K = \mathbb{Q}(\alpha)$. *Then the equations*

$$C_1: \quad \alpha^4X^4 + \alpha^3X^3 + \alpha^2X^2 + \alpha X + 1 = (\alpha - 1)Y^2 \tag{1}$$

and

$$C_2: \quad \alpha^4X^4 - \alpha^3X^3 + \alpha^2X^2 - \alpha X + 1 = (\alpha^4 - \alpha^3 + \alpha^2 - \alpha + 1)Y^2 \tag{2}$$

in $X \in \mathbb{Q}$, $Y \in K$ *have the only solutions*

$$(X, Y) = (1, \pm(\alpha^4+\alpha^3+\alpha^2+\alpha+1)), \left(-\frac{1}{3}, \pm\frac{3\alpha^4 + 5\alpha^3 - \alpha^2 + 3\alpha + 5}{9}\right)$$

and $(X, Y) = (1, \pm 1)$, *respectively.*

Consecutive terms - higher powers

Siksek and Stoll (2010): The only arithmetic progression in coprime integers of the form (a^2, b^2, c^2, d^5) is $(1, 1, 1, 1)$.

Hajdu-Tengely+Siksek-Stoll:

Theorem

There are no non-constant primitive arithmetic progressions with $l_i \in \{2, 5\}$ and $k \geq 4$.

Consecutive terms - higher powers

Primitivity is crucial!:

$$a^2, b^2, c^2, d \quad \rightarrow \quad ((p^2-2pq-q^2)^2, (p^2+q^2)^2, (p^2+2pq-q^2)^2, d),$$

infinitely many progressions.

Consecutive terms - higher powers

Primitivity is crucial!:

$$a^2, b^2, c^2, d \quad \to \quad ((p^2{-}2pq{-}q^2)^2, (p^2{+}q^2)^2, (p^2{+}2pq{-}q^2)^2, d),$$

infinitely many progressions.

$$((d^2(p^2 - 2pq - q^2))^2, (d^2(p^2 + q^2))^2, (d^2(p^2 + 2pq - q^2))^2, d^5),$$

infinitely many progressions of the form (A^2, B^2, C^2, D^5).

Consecutive terms - in number fields

We have

$$1^2, 5^2, 7^2, 73$$

and

$$7^2, 13^2, 17^2, 409, 23^2,$$

a four- and five-term arithmetic progressions over $\mathbb{Q}(\sqrt{73})$ and $\mathbb{Q}(\sqrt{409})$.

Gonzáles-Jiménez and Steuding (2010), Xarles (2012), Gonzáles-Jiménez and Xarles (2013): they provided bounds and effective results over quadratic and higher order number fields.

Arithmetic progressions

k :

$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$

$24k + 1$:

$1, 25, 49, 73, 97, 121, 145, 169, 193, 217, 241, 265, 289, 313, 337, 361$

Arithmetic progressions

k :

$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$

$24k + 1$:

$1, 25, 49, 73, 97, 121, 145, 169, 193, 217, 241, 265, 289, 313, 337, 361$

Squares in k

$1, 4, 9, 16$

Squares in $24k + 1$

1, 25, 49, 121, 169, 289, 361

Arithmetic progressions

k :

$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$

$24k + 1$:

$1, 25, 49, 73, 97, 121, 145, 169, 193, 217, 241, 265, 289, 313, 337, 361$

Squares in k

$1, 4, 9, 16$

Squares in $24k + 1$

1, 25, 49, 121, 169, 289, 361

Write $P_{a,b;N}(\ell)$ for the number of ℓ-th powers among the first N terms $b, \ldots, a(N-1)+b$ of the arithmetic progression $ax+b$ $(x \geq 0, a > 0)$. Let $P_N(\ell)$ be the maximum of these values taken over all arithmetic progressions $ax+b$.

Theorem (Behrend (1946))

$r(n)$: *the maximum number of integers not exceeding n which do not contain an arithmetic progression of 3 terms. One has that* $r(n) > n^{1-c/\log(n)^{1/2}}$.

Large sets without arithmetic progressions

Theorem (Behrend (1946))

$r(n)$: *the maximum number of integers not exceeding n which do not contain an arithmetic progression of 3 terms. One has that* $r(n) > n^{1-c/\log(n)^{1/2}}$.

Theorem (Gyarmati and Ruzsa (2012))

$Q(n)$: *maximum number of the cardinalities of subsets* $A \subseteq \{1, 2, \ldots, n\}$ *for which the equation* $x^2 + y^2 = 2z^2$ *has no nontrivial solution in A. One has that* $Q(n) \geq cn/\sqrt{\log \log n}$.

Arithmetic progressions

Theorem (Szemerédi)

For every positive integer k and real number $0 < \delta \leq 1$, there exists an integer $S(k, \delta)$ such that for any integer $N \geq S(k, \delta)$, any subset $A \subset \{1, 2, \ldots, N\}$ of cardinality at least δN contains at least one arithmetic progression

$$a, a + n, a + 2n, \ldots, a + (k-1)n$$

of length k, where a, n are positive integers.

Theorem (Szemerédi)

For any constant $\delta > 0$, if N is sufficiently large, then $P_N(2) < \delta N$.

Arithmetic progressions

Theorem (Bombieri, Granville and Pintz (1992))

There are at most $c_1 N^{2/3}(\log N)^{c_2}$ *squares in any arithmetic progression* $a + iq, i = 1, \ldots, N, q \neq 0$.

Arithmetic progressions

Theorem (Bombieri, Granville and Pintz (1992))

There are at most $c_1 N^{2/3}(\log N)^{c_2}$ *squares in any arithmetic progression* $a + iq, i = 1, \ldots, N, q \neq 0$.

Five squares instead of four+genus 5 curves+Falting's theorem.

Arithmetic progressions

Theorem (Bombieri, Granville and Pintz (1992))

There are at most $c_1 N^{2/3}(\log N)^{c_2}$ *squares in any arithmetic progression* $a + iq, i = 1, \ldots, N, q \neq 0$.

Five squares instead of four+genus 5 curves+Falting's theorem.

Theorem (Bombieri and Zannier (2002))

There are at most $c_3 N^{3/5}(\log N)^{c_4}$ *squares in any arithmetic progression* $a + iq, i = 1, \ldots, N, q \neq 0$.

Arithmetic progressions

Theorem (Bombieri, Granville and Pintz (1992))

There are at most $c_1 N^{2/3}(\log N)^{c_2}$ squares in any arithmetic progression $a + iq$, $i = 1, \ldots, N$, $q \neq 0$.

Five squares instead of four+genus 5 curves+Falting's theorem.

Theorem (Bombieri and Zannier (2002))

There are at most $c_3 N^{3/5}(\log N)^{c_4}$ squares in any arithmetic progression $a + iq$, $i = 1, \ldots, N$, $q \neq 0$.

Based on B-G-P, using genus 1 curves.

Rudin conjecture: for $N \geq 6$ we have $P_N(2) = P_{24,1;N}(2) \approx \sqrt{8N/3}$.

Remark: $P_{24,1;5}(2) = 3$ and $P_{120,49;5}(2) = 4$.

Computations

Gonzáles-Jiménez and Xarles (2014): they proved that the arithmetic progression $24n+1$ is the only one, up to equivalence, that contains $P_N(2)$ squares for the values of N such that $P_N(2)$ increases in the interval $7 \leq N \leq 52$ (these are given by $N = 8, 13, 16, 23, 27, 36, 41$ and 52).

Tools:

- Elliptic curves,
- Parametrization of points on conics,
- Elliptic Chabauty's method (developed by Bruin, Flynn and Wetherell).

Computations

In the given range they computed all the arithmetic progressions such that

$$P_N(2) = P_{a,b;N}(2),$$

except in cases of the 5-tuples

- $\{0, 1, 2, 6, 10\}, \{0, 3, 5, 6, 10\}$,
- $\{0, 2, 4, 5, 11\}, \{0, 2, 5, 7, 11\}$,
- $\{0, 1, 5, 8, 11\}, \{0, 1, 6, 8, 11\}$.

New results

How to handle the remaining 5-tuples? Instead of working with genus 5 curves and quadratic number fields we try to deal with genus 2 curves and quartic number fields.

For example in case of the tuple $\{0, 1, 2, 6, 10\}$ we have

$$\begin{aligned} b &= x_0^2, \\ x + b &= x_1^2, \\ 2x + b &= x_2^2, \\ 6x + b &= x_3^2, \\ 10x + b &= x_4^2. \end{aligned}$$

Genus 2 curves

We may parametrize all variables using x_i, x_j for any $i, j \in \{0, 1, 2, 3, 4\}, i \neq j$ to obtain

$$y^2 = f(x_i, x_j),$$

where f is homogeneous degree 6 polynomial. We have

$$(i, j) \in \{(0,1),(0,2),(0,3),(0,4),(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\},$$

so we may obtain 10 genus 2 curves.

i	j	$f(x_i, x_j)$
0	1	$-\left(9\,x_0^2 - 10\,x_1^2\right)\left(5\,x_0^2 - 6\,x_1^2\right)\left(x_0^2 - 2\,x_1^2\right)$
0	2	$\frac{1}{2}\left(4\,x_0^2 - 5\,x_2^2\right)\left(2\,x_0^2 - 3\,x_2^2\right)\left(x_0^2 + x_2^2\right)$
0	3	$-\frac{1}{54}\left(5\,x_0^2 + x_3^2\right)\left(2\,x_0^2 + x_3^2\right)\left(2\,x_0^2 - 5\,x_3^2\right)$
0	4	$\frac{1}{250}\left(9\,x_0^2 + x_4^2\right)\left(4\,x_0^2 + x_4^2\right)\left(2\,x_0^2 + 3\,x_4^2\right)$
1	2	$\left(8\,x_1^2 - 9\,x_2^2\right)\left(4\,x_1^2 - 5\,x_2^2\right)\left(2\,x_1^2 - x_2^2\right)$
1	3	$-\frac{1}{125}\left(6\,x_1^2 - x_3^2\right)\left(4\,x_1^2 + x_3^2\right)\left(4\,x_1^2 - 9\,x_3^2\right)$
1	4	$\frac{1}{729}\left(10\,x_1^2 - x_4^2\right)\left(8\,x_1^2 + x_4^2\right)\left(4\,x_1^2 + 5\,x_4^2\right)$
2	3	$-\frac{1}{8}\left(5\,x_2^2 - x_3^2\right)\left(3\,x_2^2 - x_3^2\right)\left(x_2^2 - 2\,x_3^2\right)$
2	4	$\frac{1}{64}\left(9\,x_2^2 - x_4^2\right)\left(5\,x_2^2 - x_4^2\right)\left(x_2^2 + x_4^2\right)$
3	4	$\frac{1}{8}\left(9\,x_3^2 - 5\,x_4^2\right)\left(5\,x_3^2 - 3\,x_4^2\right)\left(2\,x_3^2 - x_4^2\right)$

Our choice: $i = 2, j = 4$:

$$y_0^2 = \frac{1}{64}\left(9\,x_2^2 - x_4^2\right)\left(5\,x_2^2 - x_4^2\right)\left(x_2^2 + x_4^2\right),$$

it can be written as follows

$$C: \quad y^2 = x^6 - 13x^4 + 31x^2 + 45.$$

Based on Stoll's papers one computes that the rank of the Jacobian is 2, therefore classical Chabauty's method cannot be applied to determine the set of rational points.

Elliptic Chabauty's method

Put $K = \mathbb{Q}(\alpha)$, where $\alpha^4 - 8\alpha^2 + 36 = 0$. Over the number field K we have

$$y^2 = f_1(x) f_2(x),$$

where $\deg f_1 = 2, \deg f_2 = 4$ and

$$\begin{aligned} f_1(x) &= x^2 + \frac{1}{6}(\alpha^3 - 8\alpha)x + \frac{1}{2}(-\alpha^2 + 4), \\ f_2(x) &= x^4 + \frac{1}{6}(-\alpha^3 + 8\alpha)x^3 + \frac{1}{2}(-\alpha^2 - 14)x^2 + \\ &\quad + \frac{1}{2}(3\alpha^3 - 24\alpha)x + \frac{1}{2}(9\alpha^2 - 36). \end{aligned}$$

Elliptic Chabauty's method

We can write that

$$y_1^2 = \delta f_1(x) \text{ and } y_2^2 = \delta f_2(x),$$

where δ is an element of a finite set, in our case a set of cardinality 32. In all cases the equation $y_2^2 = \delta f_2(x)$ defines an elliptic curve over K with Mordell-Weil rank 0,1 or 2. So the rank is less than the degree of K, therefore elliptic curve Chabauty's method can be applied.

Elliptic Chabauty's method

The case of $\delta = 1/12(\alpha^3 - 2\alpha)$. The curve $y_2^2 = \delta f_2(x)$ has the model

$$E: \qquad Y^2 = X^3 + \frac{1}{4}(3\alpha^3 + \alpha^2 - 24\alpha + 50)X^2 + \\ + \frac{1}{4}(25\alpha^3 - 30\alpha^2 - 218\alpha + 408)X + \frac{1}{2}(33\alpha^3 - 90\alpha^2 - 210\alpha + 648).$$

The torsion subgroup of the Mordell-Weil group of E has 4 elements and the rank of the Mordell-Weil group is 2. The points coming from this case on C are

$$(\pm 3, 0), (-2, \pm 5), (2, \pm 5).$$

Working asymptotically

Fix any exponent $\ell \geq 2$. Let a be a positive integer (the difference of our progression), b be an integer, and put

$$S_{a,b}(\ell) = \lim_{N\to\infty} \frac{|\{x : ax + b \text{ is an } \ell\text{-th power, } 0 \leq x < N\}|}{\sqrt[\ell]{N}}.$$

We let

$$S_a(\ell) = \max_{b\in\mathbb{Z}} S_{a,b}(\ell).$$

Note that clearly, $S_{a,b}(\ell)$ does not actually depend on b, only on the residue class of b modulo a.

$$(24k - 23 \sim 24k + 1 \sim 24k + 25).$$

Working asymptotically

Set

$$S(\ell) = \max_{a \in \mathbb{N}} S_a(\ell).$$

It is not that obvious that this maximum also exists. Let $\ell \geq 2$ and let $ax + b$ be an arithmetic progression. By an ℓ-transformation of this progression we mean an arithmetic progression of the shape

$$(az^\ell)x + (b + ta)z^\ell,$$

where z is a positive integer and t is an arbitrary integer.

Main result

Theorem (Part 1)

$S(\ell)$ exists for any $\ell \geq 2$ and we have

$$S(\ell) = \begin{cases} \sqrt{\frac{8}{3}}, & \text{if } \ell = 2, \\ \displaystyle\prod_{\substack{p \text{ prime},\ p-1 \mid \ell, \\ \frac{\log p}{\log p - \log(p-1)} > \ell}} (p-1)p^{\frac{1}{\ell}-1}, & \text{otherwise.} \end{cases}$$

Main result

Theorem (Part 2)

Further, for the arithmetic progression $ax+b$ *we have* $S_{a,b}(\ell) = S(\ell)$ *if and only if it is an* ℓ*-transformation of*

$$a^*x + b^*$$

with

$$a^* = \begin{cases} 24, & \text{if } \ell = 2, \\ 5 \text{ or } 80, & \text{if } \ell = 4, \\ \prod\limits_{\substack{p \text{ prime},\ p-1 \mid \ell, \\ \frac{\log p}{\log p - \log(p-1)} > \ell}} p, & \text{otherwise,} \end{cases}$$

and

$$b^* = \begin{cases} 0, & \text{if } a^* = 1, \\ 1, & \text{otherwise.} \end{cases}$$

Remark

Note that clearly, we could take $b^* = 1$ for $a^* = 1$ as well. Our choice for b^* in the theorem in this case is just to keep the convention $0 \leq b^* < a^*$.

Observe that for ℓ odd, the products in the statement are empty, so we have

$$S(\ell) = a^* = 1$$

in this case. That is, for odd values of ℓ, the 'best' progression (in the above sense) is the trivial one x, or any of its ℓ-transformations. On the other hand, there are infinitely many even values of ℓ with $S(\ell) > 1$ and $a^* > 1$. For example, taking $\ell = p - 1$ with any odd prime p, a simple calculation shows that $p \mid a^*$ and $S(\ell) \geq \ell(\ell+1)^{\frac{1}{\ell}-1} > 1$.

Special case: $\ell = 4$

In case of $\ell = 4$ none of the two 'best' progressions is 'better' then the other. In fact, though

$$|P_{5,1;N}(4) - P_{80,1;N}(4)| \leq 1$$

for any N,

$$P_{5,1;N}(4) - P_{80,1;N}(4)$$

changes sign infinitely often.

$P_{5,1;N}(4)$	1	2	2	3	3	3	4	4	5	6	6	7	7	7
$P_{80,1;N}(4)$	1	1	2	2	3	4	4	5	5	5	6	6	7	8

Problems

Problem 1

Is it true that

$$\lim_{\ell \to \infty} S(\ell) = 1 \text{ ?}$$

Problem 2

For fixed $\ell \geq 2$, for any arithmetic progression $ax + b$ and $N \geq 1$ set

$$P_{a,b;N}(\ell) = |\{x : ax + b \text{ is an } \ell\text{-th power},\ 0 \leq x < N\}|.$$

Is it true that there exists an N_0 such that for any $N > N_0$

$$\max_{a>0,\ b\geq 0} P_{a,b;N}(\ell) = P_{a^*,b^*;N}(\ell)$$

holds? Here for the special case $\ell = 4$ we use the convention that

$$P_{a^*,b^*;N}(4) = \max(P_{5,1;N}(4), P_{80,1;N}(4)).$$

Problem 3

Use the notation from Problem 2, and for ℓ odd and $N \geq 1$ let $b^{\times}$ be the largest ℓ-th power being at most $(N-1)/2$, that is

$$b^{\times} = \left\lfloor \sqrt[\ell]{\frac{N-1}{2}} \right\rfloor .$$

Is it true that for any odd ℓ there exists an N_0 such that for any $N > N_0$

$$\max_{a>0,\ b\in\mathbb{Z}} P_{a,b;N}(\ell) = P_{1,-b^{\times};N}(\ell)$$

holds?

Sketch of the proof

Lemma (Niven, Zuckerman and Montgomery)

Let ℓ and n be positive integers greater than one, and write $U_\ell(n)$ for the number of ℓ-th roots of unity modulo n. Further, let $\nu_p(\ell)$ denote the exponent of a prime p in the factorization of ℓ.

i) *We have $U_\ell(2) = 1$, and if ℓ is odd, then $U_\ell(2^\alpha) = 1$ for any $\alpha \geq 1$. If ℓ is even, then we have $U_\ell(2^\alpha) = 2^{\min(\nu_2(\ell)+1, \alpha-1)}$ for any $\alpha \geq 2$.*

ii) *Let p be an odd prime. Then for any $\alpha \geq 1$ we have $U_\ell(p^\alpha) = p^{\min(\nu_p(\ell), \alpha-1)} \gcd(\ell, p-1)$.*

Sketch of the proof

The total number of ℓ-th powers between the first term b and the N-th term $a(N-1)+b$ of the progression $ax+b$ $(x \geq 0)$ is clearly $\sqrt[\ell]{aN}+o(1)$. The question is that how many of these (roughly) $\sqrt[\ell]{aN}$ ℓ-th powers belong to the progression $ax+b$, for a given b. Obviously, any ℓ-th power belongs to *some* progression $ax+b$ with $0 \leq b < a$.

Clearly, those ℓ-th powers u^ℓ will belong to the progression $ax+b$ for which

$$u^\ell \equiv b \pmod{a}.$$

Sketch of the proof

That is, we should find the b for which

$$M_{a,b}(\ell) := |\{u : 0 \le u < a,\ u^\ell \equiv b \pmod{a}\}|$$

is maximal. Write

$$M_a(\ell) = \max_{0 \le b < a} M_{a,b}(\ell)$$

for this maximum.

Sketch of the proof

$S_a(\ell)$ and $M_a(\ell)$ are multiplicative in a : if $a = a_1 a_2$ with $\gcd(a_1, a_2) = 1$, then

$$M_a(\ell) = M_{a_1}(\ell) M_{a_2}(\ell), \quad S_a(\ell) = S_{a_1}(\ell) S_{a_2}(\ell).$$

We may restrict our attention to arithmetic progressions $ax + b$ with $a = p^\alpha$ and

$$S_{p^\alpha, b}(\ell) \geq 1.$$

Sketch of the proof

For any b with $0 \leq b < p^\alpha$, by the definition of $M_{p^\alpha,b}(\ell)$ there exist integers

$$0 \leq u_1 < \cdots < u_{M_{p^\alpha,b}(\ell)} < p^\alpha$$

such that

$$u_1^\ell \equiv \cdots \equiv u_{M_{p^\alpha,b}(\ell)}^\ell \equiv b \pmod{p^\alpha}.$$

Sketch of the proof

We only consider the case with $p \nmid b$.

Multiplying the sequence of congruences with $u_1^{-\ell}$ modulo p^α, we see that $M_{p^\alpha,b}(\ell) = M_{p^\alpha,1}(\ell)$. So for any b with $p \nmid b$ Lemma N-Z-M shows that

$$S_{p^\alpha,b}(\ell) = \begin{cases} 2^{\alpha\left(\frac{1}{\ell}-1\right)}, & \text{if } p = 2 \text{ and } \ell \text{ is odd,} \\ 2^{\min(\nu_2(\ell)+1,\alpha-1)} \cdot 2^{\alpha\left(\frac{1}{\ell}-1\right)}, & \text{if } p = 2 \text{ and } \ell \text{ is even,} \\ p^{\min(\nu_p(\ell),\alpha-1)} \gcd(\ell, p-1) \cdot p^{\alpha\left(\frac{1}{\ell}-1\right)}, & \text{if } p \text{ is an odd prime.} \end{cases}$$

Sketch of the proof

Take $p = 2$. We have that ℓ is even, $\alpha > 1$ and

$$\min(\nu_2(\ell) + 1, \alpha - 1) + \alpha \left(\frac{1}{\ell} - 1 \right) \geq 0.$$

If

$$\nu_2(\ell) + 1 \geq \alpha - 1$$

then on the one hand

$$\ell \geq 2^{\alpha - 2},$$

and on the other hand, by the inequality

$$\alpha \geq \ell.$$

Hence we get that

$$(p^\alpha, \ell) = (4, 2),\ (8, 2),\ (16, 4).$$

Sketch of the proof

Otherwise, if

$$\nu_2(\ell) + 1 < \alpha - 1$$

then as the inequality implies

$$\nu_2(\ell) + \frac{\alpha}{\ell} \geq \alpha - 1,$$

we get $\alpha > \ell$. As $\ell \geq 2^{\nu_2(\ell)}$ this gives

$$\nu_2(\ell) < \frac{\log \alpha}{\log 2}.$$

It follows that

$$(p^\alpha, \ell) = (16, 2).$$

Computations - cubes

How to determine the 'best' progressions?

There exists integers n_0, n_1, n_2, n_3 with $0 \leq n_0 < n_1 < n_2 < n_3 < N$ such that

$$an_i + b = x_i^3 \quad (i = 0, 1, 2, 3) \tag{3}$$

with some integers x_0, x_1, x_2, x_3. The system (3) yields four genus one curves of the form

$$(n_j - n_i)X^3 + (n_i - n_k)Y^3 + (n_k - n_j)Z^3 = 0, \tag{4}$$

where $0 \leq i < j < k \leq 3$.

Computations - cubes

We get three genus one curves as follows:

$$\begin{array}{rcl} C_1: \quad n_1x_2^3 - n_2x_1^3 + (n_2 - n_1)x_0^3 & = & 0, \\ C_2: \quad n_1x_3^3 - n_3x_1^3 + (n_3 - n_1)x_0^3 & = & 0, \\ C_3: \quad n_2x_3^3 - n_3x_2^3 + (n_3 - n_2)x_0^3 & = & 0. \end{array}$$

Define morphisms

$$\begin{array}{rcl} \zeta_0 : (x_0 : x_1 : x_2 : x_3) & \to & (\zeta x_0 : x_1 : x_2 : x_3), \\ \zeta_1 : (x_0 : x_1 : x_2 : x_3) & \to & (x_0 : \zeta x_1 : x_2 : x_3), \\ \zeta_2 : (x_0 : x_1 : x_2 : x_3) & \to & (x_0 : x_1 : \zeta x_2 : x_3), \\ \zeta_3 : (x_0 : x_1 : x_2 : x_3) & \to & (x_0 : x_1 : x_2 : \zeta x_3), \end{array}$$

where ζ denotes a primitive cube root of unity. We will use subgroups of the form $H_{i,j} = \langle \zeta_0\zeta_i, \zeta_0\zeta_j \rangle$ with $1 \leq i < j \leq 3$.

Computations - cubes

For example, if we take the first two genus one curves C_1 and C_2 defined above with the subgroup $H_{1,2} = \langle \zeta_0\zeta_1, \zeta_0\zeta_2 \rangle$, then the corresponding quotient is isomorphic to the genus two hyperelliptic curve given by

$$C^{1,2}_{H_{1,2}}: \quad y^2 = ((n_2 - n_1)(n_3 - n_1)n_3)^2 x^6 + \\ +2((n_3 - n_1)n_3)^2(2n_1n_2 - n_1n_3 - n_2n_3)x^3 + ((n_3 - n_1)n_3^2)^2.$$

We note that $(1, (n_3 - n_1)(n_1 + n_2 - n_3)n_3)$ is a point on $C^{1,2}_{H_{1,2}}$.

Computations - cubes - example

We provide some details for $(n_0, n_1, n_2, n_3) = (0, 1, 3, 8)$. We obtain the three genus one curves

$$\begin{aligned} C_1 : \quad x_2^3 - 3x_1^3 + 2x_0^3 &= 0, \\ C_2 : \quad x_3^3 - 8x_1^3 + 7x_0^3 &= 0, \\ C_3 : \quad 3x_3^3 - 8x_2^3 + 5x_0^3 &= 0. \end{aligned}$$

We get the hyperelliptic curve

$$C_{H_{1,2}}^{1,2} : y^2 = 12544x^6 - 163072x^3 + 200704,$$

which is isomorphic to

$$C' : y^2 = 784x^6 - 10192x^3 + 12544.$$

Computations - cubes - example

We get that the rank of the Jacobian of the curve is one and

$$\mathrm{Jac}(C')(\mathbb{Q}) = \langle (x^2, -112, 2), (x, 28x^3+112, 2), (x-1, 28x^3-84, 2) \rangle,$$

where the first two generators are of order three and the last generates the free part. A standard application of Chabauty's method yields that the only affine rational points on C' are given by

$$\{(0, \pm 112), (1, \pm 56)\}.$$

These points do not give rise to non-constant arithmetic progressions.

Computations - fourth powers

Let (n_0, n_1, n_2) with $0 \leq n_0 < n_1 < n_2 \leq N$ be such that

$$an_i + b = x_i^4 \quad (i = 0, 1, 2). \tag{5}$$

If n_0, n_1, n_2 is an arithmetic progression, then we get

$$x_0^4 + x_2^4 = 2x_1^4.$$

However, a classical result of Dénes implies that $x_0 = x_1 = x_2$, a contradiction.

Computations - fourth powers - example

If $(n_0, n_1, n_2) = (0, 1, 3)$ then we get

$$3x_1^4 - 2x_0^4 = x_2^4.$$

The pairwise coprime integral solutions of the above equation can be parametrized by standard arguments. In our case we get

$$\begin{aligned} rx_0^2 &= -2p^2 - 2pq + q^2, \\ rx_1^2 &= 2p^2 + q^2, \\ rx_2^2 &= 2p^2 - 4pq - q^2, \end{aligned}$$

where $p, q, r \in \mathbb{Z}$ and $r \mid 12$. From the second equation we immediately get that $r > 0$.

Computations - fourth powers - example

If $r \in \{1, 3, 4, 12\}$, then the equation

$$rx_2^2 = 2p^2 - 4pq - q^2 = 6p^2 - (2p + q)^2$$

has only the trivial solution $(p, q, x_2) = (0, 0, 0)$.

Further, if $r = 2$ then the equation

$$rx_0^2 = -2p^2 - 2pq + q^2 = (q - p)^2 - 3p^2$$

has only the trivial solution.

Computations - fourth powers - example

So we are left with $r = 6$ as the only possibility. In this case multiplying the three equations above, after dividing by q^6 and writing $x = p/q$, $y = 36x_0x_1x_2$ we obtain the genus two hyperelliptic curve

$$D: \quad y^2 = -48x^6 + 48x^5 + 120x^4 + 60x^2 - 12x - 6.$$

Computations - fourth powers - example

We get that

$$\mathrm{Jac}(D)(\mathbb{Q}) = \langle (x^2+\frac{1}{2}, 0, 2), (x^2+x-\frac{1}{2}, 0, 2), (x^2+x+\frac{1}{4}, 12x+\frac{3}{2}, 2)\rangle,$$

where the first two elements are of order two and the last one generates the free part. Classical Chabauty's method implies that

$$D(\mathbb{Q}) = \{(-\frac{1}{2}, \pm\frac{9}{2})\}.$$

This gives rise to the trivial solution with $(x_0^4, x_1^4, x_2^4) = (1, 1, 1)$.

Binomial coefficients

Consider the equation

$$\binom{n}{k} = \binom{m}{l} + d.$$

There are many nice results related to $d = 0$ and

$$(k, l) = (2, 3),\ (2, 4),\ (2, 6),\ (2, 8),\ (3, 4),\ (3, 6),\ (4, 6),\ (4, 8).$$

Elliptic curves appear all in the above cases.

Cases with $d = 0$

$$\binom{16}{2} = \binom{10}{3}, \quad \binom{56}{2} = \binom{22}{3}, \quad \binom{120}{2} = \binom{36}{3},$$
$$\binom{21}{2} = \binom{10}{4}, \quad \binom{153}{2} = \binom{19}{5}, \quad \binom{78}{2} = \binom{15}{5} = \binom{14}{6},$$
$$\binom{221}{2} = \binom{17}{8}, \quad \binom{F_{2i+2}F_{2i+3}}{F_{2i}F_{2i+3}} = \binom{F_{2i+2}F_{2i+3}-1}{F_{2i}F_{2i+3}+1} \text{ for } i = 1, 2, \ldots,$$

where F_n is the nth Fibonacci number. The infinite family of solutions involving Fibonacci numbers was found by Lind and Singmaster.

Cases with $d \neq 0$

In 2017 Blokhuis, Brouwer and de Weger determined all non-trivial solutions with $d = 1$ in almost all elliptic curve cases.

n	k	m	l
11	2	8	3
60	2	23	3
160403633	2	425779	3
6	3	7	2
7	3	9	2
16	3	34	2
27	3	77	2
29	3	86	2
34	3	21	4

n	k	m	l
19630	3	1587767	2
12	4	32	2
93	4	2417	2
10	5	23	2
22	5	230	2
62	5	3598	2
135	5	26333	2
139	5	28358	2
28	11	6554	2

Cases with d as a variable

If d is not fixed Blokhuis, Brouwer and de Weger also obtained some interesting infinite families, an example is given by

$$\binom{12x^2-12x+3}{3}+\binom{x}{2}=\binom{24x^3-36x^2+15x-1}{2}.$$

In 2019, Katsipis completely resolved the case with $(k,l)=(8,2)$ and he also determined the integral solutions if $(k,l),(l,k)=(3,6)$ and $d=1$.

Let

$$C_d: \; y^2 = 15x(x-1)(x-2)(x-3)(x-4) + 15^2(8d+1)$$

and write $J_d := \mathrm{Jac}(C_d)$. The curve C_d is isomorphic to the curve defined by the equation $\binom{y}{2} = \binom{x}{5} + d$. We computed upper bounds for the numbers $r_d = \mathrm{rank} J_d(\mathbb{Q})$ using the Magma procedure `RankBound`.

Ranks of curves

We obtained the following data

i	the value of d such that $r_d \leq i$
0	$-45, -40, -39, -37, -34, -10, -9, -4, 8, 25, 26, 40, 47$
1	$-47, -36, -33, -31, -28, -26, -25, -22, -14, -13, -8, -5, -2, 5,$ $11, 17, 20, 29, 32, 41, 50$
2	$-50, -46, -41, -38, -32, -30, -29, -24, -23, -19, -16, -7, 4, 13$ $14, 23, 30, 31, 38, 43, 44$
3	$-48, -44, -43, -42, -35, -21, -20, -15, -11, -3, -1, 2, 7, 16, 18$ $19, 33, 35, 39, 42, 48$
4	$-49, -27, -18, -17, -12, -6, 9, 12, 22, 24, 34, 37, 46, 49$
5	$27, 36$
6	$0, 1, 3, 6, 10, 15, 45$
7	$21, 28$

Rank 8 curve

We also looked for high rank Jacobians for further values of d of the form $\binom{w}{2}$. For $d = 66 = \binom{12}{2}$ we obtained the equality $r_{66} = 8$:

$$< x - 3, -345 >, < x - 1, -345 >, < x - 4, 345 >, < x, 345 >,$$
$$< x + 3, 285 >, < x + 4, 135 >, < x - 11, 975 >, < x^2 + x + 30, -30x + 165 > .$$

Problem

Prove that the only solutions in positive integers of the equation $\binom{y}{2} = \binom{x}{5} + 66$ are

$$(x, y) = (1, 23), (2, 23), (3, 23), (4, 23), (11, 65), (28, 887),$$
$$(7935, 1447264765), (7939, 1449089815).$$

Large solutions

The large points are explained by the fact that on the curve $C_{\binom{w}{2}}$ we have the following solutions

$$\begin{aligned} x &= 3 \cdot 5 \cdot (2w-1)^2, \\ y &= 75(720w^4 - 1440w^3 + 1020w^2 - 300w + 31)(2w-1) \text{ and} \\ x &= 3 \cdot 5 \cdot (2w-1)^2 + 4, \\ y &= 75(720w^4 - 1440w^3 + 1140w^2 - 420w + 61)(2w-1). \end{aligned}$$

Large rank

We obtain the following divisors on $J_{\binom{w}{2}}(\mathbb{Q})$

$$
\begin{aligned}
&< x, 30w - 15, 1 >,\\
&< x - 1, 30w - 15, 1 >,\\
&< x - 2, 30w - 15, 1 >,\\
&< x - 3, 30w - 15, 1 >,\\
&< x - 4, 30w - 15, 1 >,\\
&< x - 60w^2 + 60w - 15, 108000w^5 - 270000w^4 + 261000w^3 - 121500w^2 + 27150w - 2325, 1 >,\\
&< x - 60w^2 + 60w - 19, 108000w^5 - 270000w^4 + 279000w^3 - 148500w^2 + 40650w - 4575, 1 > .
\end{aligned}
$$

$w = 9, 11 \rightarrow \text{rank} = 5$

$w = 3, 4, 5, 6, 10 \rightarrow \text{rank} = 6$

$w = 7, 8 \rightarrow \text{rank} = 7$

Numerical experiment

We computed the set

$$D_k := \left\{ \binom{n}{k} - \binom{m}{k} : \ k < m < n \leq 10^4 \right\}.$$

As one may expect, in case $k = 3$ the number of duplicates is large.

Problem

For each $N \in \mathbb{N}$ there exists $d_N \in \mathbb{N}$ such that the equation $\binom{n}{3} - \binom{m}{3} = d_N$ has at least N positive integer solutions.

D_k for $k = 5$ and 6

For $k = 5$ we found 4 values of d which appeared at least 2 times in D_5 :

$$\begin{aligned}
d &= 146438643 & (n, m) &= (117, 78), (133, 118), \\
d &= 153852348 & (n, m) &= (118, 78), (133, 117), \\
d &= 817514347 & (n, m) &= (160, 53), (209, 197), \\
d &= 2346409884 & (n, m) &= (197, 53), (209, 160).
\end{aligned}$$

For $k = 6$ we also found 4 values of d which appeared at least 2 times in D_6 :

$$\begin{aligned}
d &= 3819816 & (n, m) &= (40, 18), (57, 56), \\
d &= 32449872 & (n, m) &= (56, 18), (57, 40), \\
d &= 66273157776 & (n, m) &= (193, 66), (252, 243), \\
d &= 268624373556 & (n, m) &= (243, 66), (252, 193).
\end{aligned}$$

Genus 2 cases

Among the solutions given by Blokhuis, Brouwer and de Weger there are some with $(k, l) = (2, 5)$ e.g.:

$$\binom{10}{5} + 1 = \binom{23}{2}, \quad \binom{22}{5} + 1 = \binom{230}{2}, \quad \binom{62}{5} + 1 = \binom{3598}{2}$$

in these cases the problem can be reduced to genus 2 curves.

Genus 2 cases

Gallegos-Ruiz, Katsipis, Ulas and T.

All integral solutions (n, m) of equation $\binom{n}{k} = \binom{m}{l} + d$ with $d \in \{-3, \ldots, 3\}$, $k = 2$, $l = 5$ are as follows.

d	solutions
-3	$[(3,6)]$
-2	$[]$
-1	$[(11,8)]$
0	$[(2,5),(4,6),(7,7),(78,15),(153,19)]$
1	$[(23,10),(230,22),(3598,62),(26333,135),(28358,139)]$
2	$[(3,5)]$
3	$[(31,11),(94,16),(346888,375),(356263,379)]$

About the proof

In case of $d = 3$ the hyperelliptic curve is given by

$$y^2 = 15x(x-1)(x-2)(x-3)(x-4) + 75^2$$

and the rank of the Jacobian is 6. A Mordell-Weil basis is as follows (in Mumford representation)

$$D_1 =< x-4, -75 >, D_2 =< x-3, 75 >,$$
$$D_3 =< x-1, -75 >, D_4 =< x, 75 >,$$
$$D_5 =< x^2 - 7x + 30, 195 >, D_6 =< x^2 - 3x + 20, -30x - 45 > .$$

About the proof

We apply Baker's method to get a large upper bound for $\log|x|$, in this case we obtain

$$\log|x| \leq 1.028 \times 10^{612}.$$

Every integral point on the curve can be expressed in the form

$$P - \infty = \sum_{i=1}^{6} n_i D_i$$

with $||(n_1, n_2, n_3, n_4, n_5, n_6)|| \leq 1.92 \times 10^{306}$.

Hyperelliptic logarithm method

We choose to compute the period matrix and the hyperelliptic logarithms with 1500 digits of precision. The hyperelliptic logarithms of the divisors D_i are given by

$$
\begin{aligned}
\varphi(D_1) &= (0.087945\ldots + i0.112834\ldots, -0.473844\ldots - i0.741784\ldots) \in \mathbb{C}^2,\\
\varphi(D_2) &= (0.114612\ldots + i0.112834\ldots, -0.420527\ldots - i0.741784\ldots) \in \mathbb{C}^2,\\
\varphi(D_3) &= (-0.044486\ldots + i1.333456\ldots, -0.416321\ldots + i5.329970\ldots) \in \mathbb{C}^2,\\
\varphi(D_4) &= (0.127905\ldots + i0.112834\ldots, -0.413878\ldots - i0.741784\ldots) \in \mathbb{C}^2,\\
\varphi(D_5) &= (-0.118415\ldots + i0.037611\ldots, -0.857076\ldots - i0.247261\ldots) \in \mathbb{C}^2,\\
\varphi(D_6) &= (0.128537\ldots + i0.075223\ldots, -0.173077\ldots - i0.494522\ldots) \in \mathbb{C}^2.
\end{aligned}
$$

Hyperelliptic logarithm method

Setting $K = 10^{1300}$ we get a new bound 125.87 for $||(n_1, n_2, n_3, n_4, n_5, n_6)||$. We repeat the reduction process with $K = 10^{18}$ that yields a better bound, namely 15.99. Three more steps with $K = 10^{15}, K = 10^{13}$ and $K = 6 \times 10^{11}$ provide the bounds $14.85, 14.1$ and 13.8. It remains to compute all possible expressions of the form

$$n_1 D_1 + \ldots + n_6 D_6$$

with $||(n_1, n_2, n_3, n_4, n_5, n_6)|| \leq 13.8$. We performed a parallel computation to enumerate linear combinations coming from integral points on a machine having 12 cores. The computation took 3 hours and 23 minutes.

Solutions

We obtained the following non-trivial solutions with $n \geq 5$

$$\begin{aligned}
\binom{11}{5} + 3 &= \binom{31}{2}, \\
\binom{16}{5} + 3 &= \binom{94}{2}, \\
\binom{375}{5} + 3 &= \binom{346888}{2}, \\
\binom{379}{5} + 3 &= \binom{356263}{2}.
\end{aligned}$$

Genus 3 cases

In case of the equation $\binom{n}{2} = \binom{m}{7} + d$ one obtains genus 3 curves. Stoll proved that the rank of the Jacobian is 9 if $d = 0$. For other values of d in the range $\{-3, \ldots, 3\}$ many of the genus 3 hyperelliptic curves have high ranks as well. Balakrishnan et. al. developed an algorithm to deal with genus 3 hyperelliptic curves defined over $\mathbb{Q}$ whose Jacobians have Mordell-Weil rank 1. If $d = -2$, then the equation is isomorphic to the curve

$$Y^2 = 70X^7 - 1470X^6 + 12250X^5 - 51450X^4 + 113680X^3 - 123480X^2 + 50400X - 661500$$

and using Magma (with `SetClassGroupBounds("GRH")` to speed up computation) we get that the rank of the Jacobian is 1. The affine points are $(8, \pm 1470)$, hence we have the solution $\binom{4}{2} = \binom{8}{7} - 2$.