On Diophantine graphs

G. Batta

University of Debrecen

Number Theory Seminar

Plan of the talk

- Introduction
- Extendability of Diophantine graphs
- Bounds for the number of edges in Diophantine graphs:
  - lower bounds
  - upper bounds
- Chromatic number of Diophantine graphs
- Remarks and open problems

The presented new results are joint with **L. Hajdu, A. Pongrácz.**

Introduction

A **Diophantine n-tuple** is a set $\{a_1, \ldots, a_n\}$ of distinct positive integers if $a_i a_j + 1$ is a square ($1 \le i < j \le n$).

Fermat: $\{1, 3, 8, 120\}$ is a Diophantine quadruple

Baker and Davenport: $\{1, 3, 8\}$ can be extended to a Diophantine quadruple only by adjoining 120. Thus $\{1, 3, 8\}$ cannot be extended to a Diophantine quintuple.

Dujella and Pethő: already the pair $\{1, 3\}$ cannot be extended to a Diophantine quintuple

Dujella: there are no Diophantine sextuples and there are only finitely many Diophantine quintuples

He, Togbé and Ziegler: there are no Diophantine quintuples

Introduction

We study **Diophantine graphs**.

Let $V \subseteq \mathbb{N}$. The **induced Diophantine graph** $D(V)$ has vertex set V, and two numbers in V are linked by an edge if and only if their product increased by one is a square.

A finite graph G is a **Diophantine graph** if it is isomorphic to $D(V)$ for some finite set $V \subseteq \mathbb{N}$. Then $D(V)$ is a **representation** of G as a Diophantine graph.

Introduction

Studying properties of integers through graphs has a long tradition.

J. A. Gallian, *A Dynamic Survey of Graph Labeling, Twenty-sixth edition, December 1, 2023*, Electronic J. Combin. #DS6, (1998): 7 sections, 65 subsections, 3295 references.

One example:

- Arithmetic graphs: two integers are linked if and only if their difference is divisible only by primes coming from a fixed finite set. (Results of **Győry, Ruzsa, Tijdeman, Ćustić, Kreso, Hajdu** and others, also in the algebraic case.)

Some of the main directions of research: representability and structural questions, edge density, important applications.

Introduction

The results mentioned describe **complete** Diophantine graphs.
He, Togbé and Ziegler: K_5 is a 'forbidden' subgraph.

Dujella: upper bounds for the number of the K_t subgraphs of $D(V_N)$ for $2 \leq t \leq 4$ and $V_N = \{1, \ldots, N\}$. (Motivation: study Diophantine pairs, triples and quadruples in $\{1, \ldots, N\}$.)

Bugeaud and Gyarmati: (beside several other interesting results, e.g. for higher and mixed powers) the number of edges in a Diophantine graph on N vertices is bounded by $0.4N^2$.

Yip: recent results for bipartite Diophantine graphs for higher powers

Note that the cases $k = 2$ and $k \geq 3$ are rather different in nature.
A strong warning is the following open problem:

Dujella: Is $K_{3,3}$ Diophantine?

Extendability of Diophantine graphs

We start with the question of **extensions of Diophantine graphs**: given $D(V)$, we would like to **attach a new vertex**, linked to some **prescribed old vertices**.

As we will see, it is always possible to find **a new isolated vertex**, or **a vertex** which is **linked to exactly one vertex** of a given Diophantine graph $D(V)$.

In fact, there are always infinitely many appropriate positive integers to solve these problems.
To extend a Diophantine graph $D(V)$ by **a vertex which is linked to exactly two given vertices** in V is more problematic.

If the square-free parts of two different numbers $v_1, v_2 \in V$ coincide, then there are only finitely many common neighbors w of v_1, v_2 in $\mathbb{N}$.

Extendability of Diophantine graphs

Theorem 1 (G. Batta, A. Pongrácz, H (202?))

Let $V = \{v_1, \ldots, v_n\} \subseteq \mathbb{N}$. Then each of the following conditions is satisfied by infinitely many positive integers w whose square-free parts differ from that of v_k for all $1 \leq k \leq n$:

i) *w is an isolated vertex of $D(V \cup \{w\})$,*

ii) *w is linked in $D(V \cup \{w\})$ to exactly one arbitrarily prescribed vertex $v_i \in V$,*

iii) *w is linked in $D(V \cup \{w\})$ to exactly two prescribed vertices $v_i, v_j \in V$ with different square-free part.*

Extendability of Diophantine graphs

In some sense, Theorem 1 cannot be extended.

Proposition 1 (G. Batta, A. Pongrácz, H (202?))

Any three positive integers have only finitely many common neighbors in $\mathbb{N}$.

Proof of Proposition 1. If w is a neighbor of u_1, u_2, u_3, then $(u_1x+1)(u_2x+1)(u_3x+1) = y^2$ with $x = w$ and some $y \in \mathbb{N}$.

Baker: there are only finitely many integer points on elliptic curves - and we are done. $\square$

$1, 2, 3$ do not have common neighbors. This can be verified e.g. by **Magma**, by results of **Gebel, Pethő, Zimmer** and **Stroeker, Tzanakis**.

Baker and Davenport: the only common neighbor of $1, 3, 8$ is 120. As 7 is also a neighbor of 120 in $\mathbb{N}$, we cannot extend $\{1, 3, 7, 8\}$ by a new vertex that is linked to $1, 3, 8$ but not to 7.

Extendability of Diophantine graphs - proof of Thm1

Theorem 1 is an immediate consequence of the following lemmas.

Lemma 1 (G. Batta, A. Pongrácz, H (202?))

Let $v_1, \ldots, v_n$ be different positive integers. Then there exist infinitely many $w \in \mathbb{N}$ such that $v_i w + 1$ is not a square, and the square-free parts of w and v_i are different for all $i = 1, \ldots, n$.

Lemma 2 (G. Batta, A. Pongrácz, H (202?))

Let $v_1, \ldots, v_n$ be different positive integers, and let $i \in \{1, \ldots, n\}$ be fixed. Then there exist infinitely many $w \in \mathbb{N}$ such that $v_i w + 1$ is a square, $v_j w + 1$ is not a square for any $j \in \{1, \ldots, n\}$ with $j \neq i$, and the square-free part of w is different from those of the v_ℓ ($\ell = 1, \ldots, n$).

Lemma 3 (G. Batta, A. Pongrácz, H (202?))

Let $v_1, \ldots, v_n$ be different positive integers and $i, j \in \{1, \ldots, n\}$ distinct indices such that the square-free parts of v_i, v_j are different.

Then there exist infinitely many $w \in \mathbb{N}$ such that:

- $v_i w + 1$ *and* $v_j w + 1$ *are squares,*
- $v_\ell w + 1$ *is not a square for* $\ell \in \{1, \ldots, n\}, \ell \neq i, j$,
- *the square-free part of* w *is different from all those of the* v_m $(m = 1, \ldots, n)$.

Extendability of Diophantine graphs - proof of Thm1

Main idea of the proof of Lemma 1., 2., and 3. In each case, the proof is based on examining the cardinality of the solution sets of various Diophantine equations.

Thus, in the Lemma 1., CRT implies that there are infinitely many solutions.

In the case of Lemma 2., we compare the solution set of a system of congruences to the solution set of finitely many Pell-equations.

In the proof of Lemma 3., we compare the solution set of a Pell-equation to the solution set of finetely many simultaneous Pell-equations.

Then we verify that the square-free parts of these solutions can come from an infinite set.

Extendability of Diophantine graphs - some corollaries

Corollary 1 (G. Batta, A. Pongrácz, H (202?))

Every finite graph has a Diophantine subdivision. In particular, every finite graph is a minor of a Diophantine graph.

Sketch of the proof of Corollary 1. Let G be a finite graph with n vertices.

According to Lemma 1 we can choose a set V of n positive integers iteratively, each with a different square-free part, such that $D(V)$ is an empty graph.

Then for any edge of G, we can extend V by a new number that is linked to exactly the two endpoints of the edge in $D(V)$.

This can also be done iteratively: in each step, we choose a new number that is not linked to any number other than the two endpoints of the given edge. $\square$

Lower bounds for the number of edges

Our next theorems concern the edge density in Diophantine graphs, i.e. the number of edges $e(D(V))$ of $D(V)$ on n vertices.

In fact, we are interested in $\max_{|V|=n} e(D(V))$ $(n \in \mathbb{N})$, or its order of magnitude.

Theorem 1 implies the existence of graphs $D(V)$ with $|V| = n$ and $e(D(V)) = \Omega(n)$.

Dujella: the existence of such graphs with $e(D(V)) = \frac{6}{\pi^2} n \log n + \Theta(n)$.

In fact, **Dujella** proved this for $D(V_N)$ induced by $V_N := \{1, \ldots, N\}$.
So the asymptotic edge density of $D(V_N)$ is $\frac{6}{\pi^2} \log N$.

Lower bounds for the number of edges

Theorem 2 (G. Batta, A. Pongrácz, H (202?))

For any $\varepsilon > 0$ there exists an arbitrarily large n and a Diophantine graph $D(V)$ with n vertices such that

$$e(D(V)) > n(\log n)^{2\log 2-\varepsilon}.$$

By this statement, we see that there are Diophatine graphs on n vertices with edge density at least $(\log n)^{2\log 2-\varepsilon}$.

Lower bounds for the number of edges - proof of Thm2

In the proof we need a classical assertion (also used by **Dujella**).

Write $\omega(d)$ for the number of different prime divisors of $d \in \mathbb{N}$.

Lemma 4

Let $S(a)$ be the number of solutions of $x^2 \equiv 1 \pmod{a}$. Then $S(a) \leq 2^{\omega(a)+1}$. More precisely,

1. *if $2 \nmid a$, then $S(a) = 2^{\omega(a)}$,*
2. *if $2 \mid a$ but $4 \nmid a$, then $S(a) = 2^{\omega(a)-1}$,*
3. *if $4 \mid a$ but $8 \nmid a$, then $S(a) = 2^{\omega(a)}$, and*
4. *if $8 \mid a$, then $S(a) = 2^{\omega(a)+1}$.*

By the approach of Dujella, we can estimate the degree of vertices in $D(V_N)$.

Lemma 5 (G. Batta, A. Pongrácz, H (202?))

Let $1 \leq a \leq N$. Then the degree of a in $D(V_N)$ is at most $8\sqrt{N/a} \cdot 2^{\omega(a)}$.

As a simple consequence we get

Corollary 4 (G. Batta, A. Pongrácz, H (202?))

Let $\delta > 0$, $C > 1$ and $t \in \mathbb{N}$. Then for N large enough, the total degree in the graph $D(V_N)$ of all numbers a in the interval $[N(\log N)^{-t\delta}, N(\log N)^{-(t-1)\delta}]$ such that $\omega(a) \leq C \log\log N$ is at most $8N(\log N)^{C\log 2+\delta/2}$.

The proofs are simple but technical, so we omit them.

Sketch of the proof of Theorem 2. Since the argument is rather involved, we give an overview of our strategy.

We start out from V_N, and leave out vertices of 'small' degree to increase the edge density $\Theta(\log N)$ of the graph $D(V_N)$.

Clearly, the omission of a vertex v from a graph G increases the average degree if and only if $\deg(v)$ is less than the edge density, that is, half of the average degree in G.

Hence, the natural idea is to omit every vertex from $D(V_N)$ whose degree is less than $\frac{6}{\pi^2}\log N$.

After this, only $N/(\log N)^{c_1}$ vertices remains with some $c_1 > 0$. Thus in the graph obtained, the average degree has order of magnitude $\Theta\left((\log N)^{1+c_1}\right)$ rather than $\log N$.

Repeating the same process by omitting vertices with degree less than $(\log N)^{1+c_1}$ (approximately), the average degree increases to the order of magnitude $\Theta\left((\log N)^{1+c_2}\right)$ with some $c_2 > c_1$.

Determining the limit c of the sequence $c_1, c_2, \ldots$, we get $c = 2\log 2 - 1$.

So the rough idea is to show that for any $\varepsilon > 0$, asymptotically 100% of the $\Theta(N \log N)$ edges survive if we omit vertices from $D(V_N)$ with degree at most $(\log N)^{2\log 2-\varepsilon}$, and at the same time, only about $N(\log N)^{1-2\log 2+\varepsilon}$ vertices remain.

This yields a graph with edge density at least $(\log N)^{2\log 2-\varepsilon}$ rather than $\Theta(\log N)$.

Lower bounds for the number of edges - proof of Thm2

For this, we use a classical **Hardy-Ramanujan** type theorem.

The variant we need was found by **Sathe** and simplified by **Selberg**.

Let $\pi(x, k)$ denote the number of positive integers $a \leq x$ with $\omega(a) = k$.

Theorem A (Sathe-Selberg)

Let $C > 1$ be a fixed constant. Then for all $x \geq 3$ we have

$$\sum_{k > C \log \log x} \pi(x, k) \leq \frac{x}{\log x} \cdot \sum_{k > C \log \log x} \frac{(\log \log x)^{k-1}}{(k-1)!}.$$

Upper bounds for the number of edges

Our first theorem into this direction is an immediate consequence of a classical theorem of **Turán**.

Theorem 3 (G. Batta, A. Pongrácz, H (202?))

For any Diophantine graph $D(V)$ with $|V| = n$ we have

$$e(D(V)) \leq \frac{3}{8}n^2.$$

Proof of Theorem 3. By the result of **He, Togbé and Ziegler** we know that $D(V)$ cannot contain a K_5. Thus the statement is a simple consequence of **Turán's** theorem with $k = 5$. □

We note that **Adrian Beker** (a master student of **Andrej Dujella**) informed us that combining bounds for the number of extensions of Diophantine triples to quadruples by standard supersaturation results for Turán's theorem say, he can reduce the above upper bound to $\left(\frac{1}{3} + o(1)\right) n^2$.

Upper bounds for the number of edges

We strongly suspect that $\max\limits_{|V|=n} e(D(V)) = o(n^2)$ should hold.

To find a sub-linear upper estimate for the edge density of Diophantine graphs, the following question is vital:

Is $K_{t,t}$ the subgraph of a Diophantine graph for all $t \in \mathbb{N}$?

If the answer is positive, then it yields an infinite sequence of Diophantine graphs with n vertices and at least $n^2/4$ edges.

If the answer is negative, with counterexample $t_0 \in \mathbb{N}$, then by a classical result of **Kővári, Sós and Turán** there is an $O(n^{2-1/t_0})$ upper bound for the number of edges in Diophantine graphs on n vertices.

Upper bounds for the number of edges

However, this problem seems to be out of reach with state-of-the-art methods.

An open problem of **Dujella** asks whether already $K_{3,3}$ is a Diophantine graph or not.

Note that as a simple consequence of Theorem 1, we obtain that $K_{2,t}$ is a Diophantine graph for any t.

By Proposition 1 we know that any three positive integers have only finitely many common neighbors in $\mathbb{N}$. However, it is not uniform!

Upper bounds for the number of edges

We provide a stronger result in this direction.

However, for this we need to assume two deep conjectures related to elliptic curves.

The first conjecture is due to **Szpiro**.

Conjecture 1 (Szpiro)

for all $\varepsilon > 0$ *there are only finitely many elliptic curves* E *over* $\mathbb{Q}$ *satisfying*

$$\frac{\log |D_E|}{\log C_E} \geq 6 + \varepsilon,$$

where D_E *is the minimal discriminant and* C_E *is the conductor of* E.

Upper bounds for the number of edges

The second conjecture concerns the ranks of elliptic curves over $\mathbb{Q}$.

For a long time, it has been widely believed that there is no absolute bound for them.

However, recent heuristics of **Park, Poonen, Voight and Wood** suggest that possibly the opposite is true.

This has been conjectured much earlier by **Néron**.

Conjecture 2 (Néron)

The ranks of elliptic curves over $\mathbb{Q}$ *are uniformly bounded.*

We shall also need a deep result of **Hindry and Silverman.**

Let S be a finite set of primes, and let $\mathbb{Z}_S$ be the set of rationals such that (in their primitive forms) all prime factors of their denominators belong to S.

Write r_E, D_E and C_E for the rank, discriminant and conductor, respectively, of an elliptic curve E given in its minimal Weierstrass model.

Theorem B (Hindry and Silverman)

There exists an absolute constant C_0 such that the number of points on E from $\mathbb{Z}_S^2$ is at most

$$C_0^{|S|+1+(1+r_E)\frac{\log|D_E|}{\log C_E}}.$$

Upper bounds for the number of edges

Our (strongly conditional) result into this direction is the following.

Theorem 4 (G. Batta, A. Pongrácz, H (202?))

Let $a, b \in V$, and suppose that $D(V) \cong K_{t,t}$ with $t \geq 1$, such that a, b belong to the same vertex class. Then, assuming Szpiro's conjecture and Néron's conjecture, there exists a constant $C = C(\omega(ab(a-b)))$ such that $t < C$.

One can see that that C is not at all absolute, but it depends 'only' on two vertices (integers).

Sketch of the proof of Theorem 3. We may assume that $t \geq 3$.

Let c be an element from the vertex class of a, b, and d from the other vertex class.

Then with some integer r we have

$$(ad + 1)(bd + 1)(cd + 1) = r^2.$$

Do the following:

- calculate the minimal model E_0 of the elliptic curve E implied by the above equation,
- also the required invariants of E_0,
- get control on the prime factors of the denominators of the images of the integer points E on E_0.

Then our claim follows from Theorem B of **Hindry and Silverman**, assuming the conjectures of **Szpiro** and **Néron.** □

Chromatic number of Diophantine graphs

Finally, we study the chromatic number of Diophantine graphs.

As the clique number of Diophantine graphs is at most four, it is plausible to ask whether all Diophantine graphs are four-colorable.

Our next result shows that it is not the case.

Theorem 5 (G. Batta, A. Pongrácz, H (202?))

Let $V = \{1, 3, 8, 120, 2, 4, 12, 20, 24, 6, 22, 92, 204, 420, 36, 78, 84, 140, 210, 360, 364, 560, 60, 14, 40, 136, 220, 312, 33, 9, 10, 52, 56, 728, 11, 48, 90, 168, 408, 840, 5, 7, 28, 30, 34, 35, 46, 70, 88, 132, 180, 240, 2184, 280, 16, 21, 32, 44, 156, 816, 380, 13, 39, 72, 80, 96, 462, 528, 1140, 2380, 23, 102, 105, 110, 152, 264, 456, 858, 2520, 1365\}$.
Then the graph $D(V)$ *has chromatic number five.*

This 80-element set is the smallest example we know, and it is minimal.

Chromatic number of Diophantine graphs - proof of Thm5

Sketch of the proof of Theorem 5. The verification of the statement is done by an exhaustive case distinction.

The vertices are listed in a carefully chosen order, starting by the Diophantine quadruple $\{1, 3, 8, 120\}$.

At all other vertices, initially the set of all colors $\{0, 1, 2, 3\}$ is registered as possibilities.

Whenever we assign a definite color to a vertex u, the algorithm deletes that color as a possible one from the color sets at all the neighbors of u.

The program iterates through the list of vertices, always making a case distinction.

Chromatic number of Diophantine graphs - proof of Thm5

If a vertex is found that has no possible colors left, the program deletes the corresponding copy of the graph.

Initially we have chosen the 1000 positive integers a where the largest values of the function $2^{S(a)}/\sqrt{a}$ are attained (see Lemmas 4 and 5).

The program verified that this graph is not four-colorable in less than a second on an average PC.

To reduce the size, we omitted 'low-degree' vertices from this 1000-vertex graph.

Once we reduced down to a graph with 119 vertices, a certain refinement was needed.

Finally, we were left with the vertex set V given in the statement. $\square$

Remarks and open problems - Hamiltonian paths and cycles

As $a(a+2)+1=(a+1)^2$, $a, a+2 \in V_N$ are always linked.

So $D(V_N)$ is connected for $N \geq 8$: any two odd and any two even numbers are connected by paths of the form $a, a+2, a+4, \ldots$, and 1 and 8 are also linked.

This almost yields a Hamiltonian path: start from the largest odd number, walk down to 1, follow with $8, 6, 4, 2, 12$, and then keep upward. This path only avoids 10.

However, there is never a Hamiltonian cycle in $D(V_N)$: partitioning the numbers in V_N into $\pmod 4$ residue classes, the elements of the class of 2 are only linked to numbers divisible by 4.

So there is always an 'almost' Hamiltonian path, and there is never a Hamiltonian cycle in $D(V_N)$.

Remarks and open problems - Hamiltonian paths and cycles

Also, there is no Hamiltonian path in $D(V_N)$ if $N \equiv 2, 3 \pmod 4$.

In some small examples where $N \equiv 0, 1 \pmod 4$, say for $N = 17, 32, 33$, there is no Hamiltonian paths in $D(V_N)$.

However, for other small values of $N \equiv 0, 1 \pmod 4$ such paths exist, and it seems to be more and more probable as N gets larger.

There is a Hamiltonian path in $D(V_N)$ for infinitely many values of N, e.g. for $N = 16k^2$ $(k \in \mathbb{N})$.

Problem 1 (G. Batta, A. Pongrácz, H (202?))

Is there an $N_0 \in \mathbb{N}$ such that for all $N \geq N_0$, $N \equiv 0, 1 \pmod 4$ there is a Hamiltonian path in $D(V_N)$?

Remarks and open problems - representability of various graphs

Theorem 1 implies that every graph with maximum degree at most two is Diophantine.

On the other hand, as K_5 is not Diophantine, there exist non-Diophantine graphs with maximum degree k for any $k \geq 4$.

So the following question arises naturally.

Problem 2 (G. Batta, A. Pongrácz, H (202?))

Is it true that every finite graph with maximum degree at most three is Diophantine? Or equivalently, is every finite 3*-regular graph Diophantine?*

In fact, we expect a negative answer.

Remarks and open problems - representability of various graphs

The smallest 3-regular graph is K_4, which is Diophantine.

There are no 3-regular graphs on five vertices.
There are two 3-regular graphs on six vertices:

- the complement of a 6-cycle, which is Diophantine, witnessed by the representation $\{1, 3, 8, 10, 96, 168\}$,
- the complete bipartite graph $K_{3,3}$, which is the smallest open case of the problem.

Besides the pyramid graph on five vertices, $K_{3,3}$ is the smallest graph G such that it is unknown whether G is Diophantine (**Dujella**).

Problem 3 (G. Batta, A. Pongrácz, H (202?))

Is the pyramid graph Diophantine?

Remarks and open problems - representability of various graphs

Another question related to Theorem 1 is the following.

Problem 4 (G. Batta, A. Pongrácz, H (202?))

Is it true that every Diophantine graph can be represented as $D(V)$, with some V consisting of integers having pairwise different square-free parts?

Remarks and open problems - representability of various graphs

As bipartite graphs play a crucial role, we propose the following question (for which we strongly expect a negative answer).

Problem 5 (G. Batta, A. Pongrácz, H (202?))

Is $K_{t,t}$ a subgraph of a Diophantine graph for all $t \in \mathbb{N}$?

Once again, $K_{3,3}$ is the smallest open case of this problem.

We also propose a problem concerning the complexity of the language of Diophantine graphs.

Problem 6 (G. Batta, A. Pongrácz, H (202?))

Is it decidable whether an input finite graph is Diophantine?

It is well-known that the solvability of Diophantine equations is undecidable.

Remarks and open problems - chromatic numbers of Diophantine graphs

Using an approach which is similar to that in the proof of Theorem 5, we tried to find a Diophantine graph that is not five-colorable.

The complexity of this problem is orders of magnitude larger than that of the four-colorable variant.

As the edge density (and the minimum degree) of a Diophantine graph can be arbitrarily large, there is no obvious upper bound for the chromatic number of these graphs.

So we suggest the following question.

Problem 7 (G. Batta, A. Pongrácz, H (202?))

Is there a Diophantine graph that is not five-colorable? More generally, are there Diophantine graphs with arbitrarily large chromatic number?

Thank you very much for your attention!