Diophantine m-tuples and elliptic curves

Seoyoung Kim

AWM50 Women in Math Conference
SUNY Albany 04.28.2023

Do you see any pattern ?

$$\{1, 3, 8\}$$

How about this set ?

$$\{1, 3, 8, 120\}$$

Introduction of Diophantine m-tuples

A Diophantine tuple (over $\mathbb{N}$) is a set $\mathcal{D}$ of positive integers such that for any distinct elements a and b in $\mathcal{D}$, we have

$$ab + 1 = \square.$$

The previous example $\{1, 3, 8, 120\}$ is by Fermat :

The previous example $\{1, 3, 8, 120\}$ is by Fermat :
and this is the only way of extending $\{1, 3, 8\}$!

THE EQUATIONS $3x^2-2=y^2$ AND $8x^2-7=z^2$

By A. BAKER *and* H. DAVENPORT

[Received 6 November 1968]

1. THE four numbers 1, 3, 8, 120 have the property that the product of any two, increased by 1, is a perfect square. Professor J. H. van Lint, in a lecture at Oberwolfach in March 1968, discussed the problem whether there is any other positive integer that can replace 120. Since then Professor van Lint has been good enough to send us a copy of a report† in which he gives references to the history of the problem, and also gives a proof that there is no such integer up to $10^{1700000}$.

The previous example $\{1, 3, 8, 120\}$ is by Fermat :
and this is the only way of extending $\{1, 3, 8\}$!

THE EQUATIONS $3x^2-2=y^2$ AND $8x^2-7=z^2$

By A. BAKER *and* H. DAVENPORT

[Received 6 November 1968]

1. THE four numbers 1, 3, 8, 120 have the property that the product of any two, increased by 1, is a perfect square. Professor J. H. van Lint, in a lecture at Oberwolfach in March 1968, discussed the problem whether there is any other positive integer that can replace 120. Since then Professor van Lint has been good enough to send us a copy of a report† in which he gives references to the history of the problem, and also gives a proof that there is no such integer up to $10^{1700000}$.

Can you find any Diophantine quintuple ?

The previous example $\{1, 3, 8, 120\}$ is by Fermat :
and this is the only way of extending $\{1, 3, 8\}$!

THE EQUATIONS $3x^2-2=y^2$ AND $8x^2-7=z^2$

By A. BAKER *and* H. DAVENPORT

[Received 6 November 1968]

1. THE four numbers 1, 3, 8, 120 have the property that the product of any two, increased by 1, is a perfect square. Professor J. H. van Lint, in a lecture at Oberwolfach in March 1968, discussed the problem whether there is any other positive integer that can replace 120. Since then Professor van Lint has been good enough to send us a copy of a report† in which he gives references to the history of the problem, and also gives a proof that there is no such integer up to $10^{1700000}$.

Can you find any Diophantine quintuple ?
No ! (He - Togbé - Ziegler, 2019)

Diophantus of Alexandria found the first set of positive rationals having this property.

$$\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$$

Generalizations

A Diophantine tuple over F is a subset $\mathcal{D}$ of a field F such that for any distinct elements a and b in $\mathcal{D}$, we have

$$ab + 1 = \square.$$

$F = \mathbb{Q}$, we have a quintuple

$$\left\{\frac{243}{560}, \frac{1147}{5040}, \frac{1100}{63}, \frac{7820}{567}, \frac{95}{112}\right\}$$

and moreover, this can be extended

$$\left\{\frac{243}{560}, \frac{1147}{5040}, \frac{1100}{63}, \frac{7820}{567}, \frac{95}{112}, \frac{196}{45}\right\}.$$

$F = \mathbb{Q}$, we have a quintuple

$$\left\{\frac{243}{560}, \frac{1147}{5040}, \frac{1100}{63}, \frac{7820}{567}, \frac{95}{112}\right\}$$

and moreover, this can be extended

$$\left\{\frac{243}{560}, \frac{1147}{5040}, \frac{1100}{63}, \frac{7820}{567}, \frac{95}{112}, \frac{196}{45}\right\}.$$

but there is no known example of size 7.

Why is it hard to extend Diophantine tuples ?

Given a Diophantine triple {a,b,c} over a field F, extending it to a Diophantine quadruple {a,b,c,x} over F means to find $x \in F$ such that

$$ax + 1 = s^2$$
$$bx + 1 = t^2$$
$$cx + 1 = r^2$$

Given a Diophantine triple {a,b,c} over a field F, extending it to a Diophantine quadruple {a,b,c,x} over F means to find $x \in F$ such that

$$ax + 1 = s^2$$
$$bx + 1 = t^2$$
$$cx + 1 = r^2$$

$$(ax + 1)(bx + 1)(cx + 1) = (str)^2$$

Hence, extending a Diophantine triple to a quadruple is as hard as finding such $x \in F$!

Why elliptic curves ?

An elliptic curve (over $\mathbb{Q}$) is the set of solutions to an equation of the form

$$E : y^2 = x^3 + Ax^2 + Bx + C, \quad \text{where } A, B, C \in \mathbb{Q}.$$

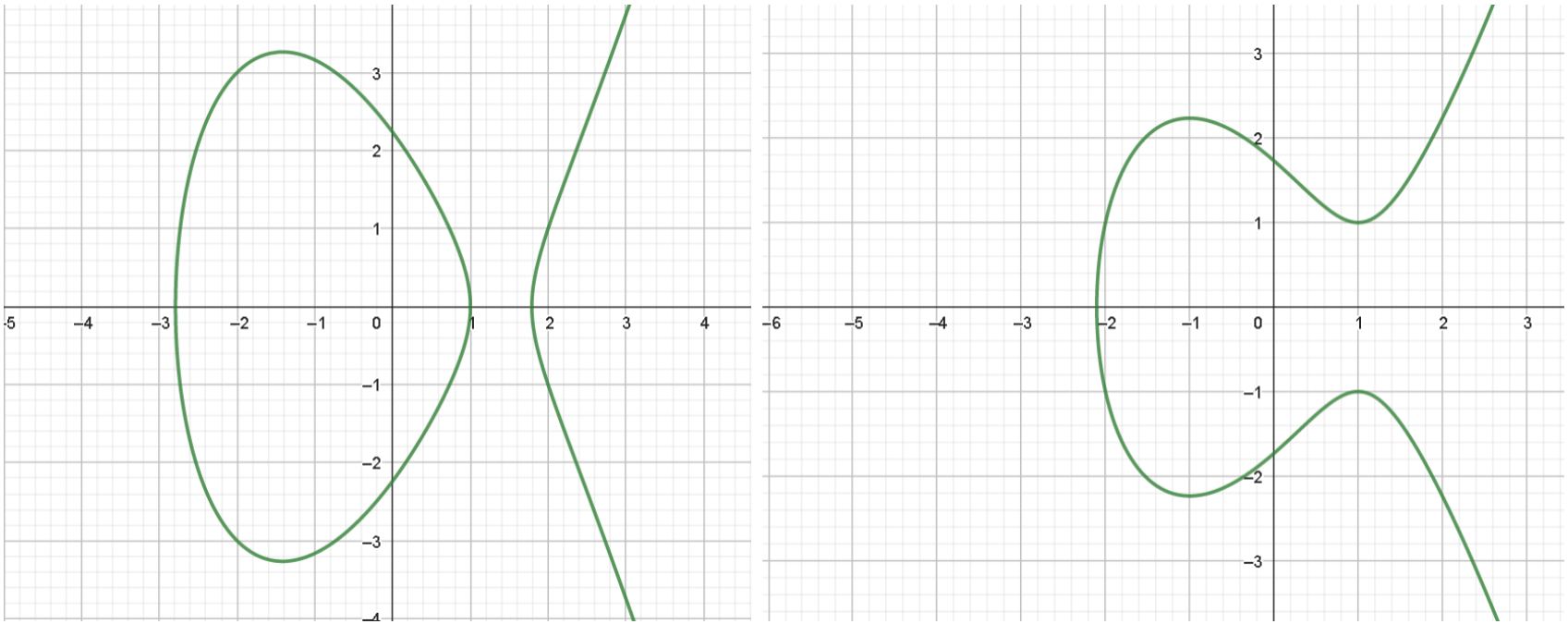


Figure – Graph of $y^2 = x^3 - 6x + 5$ and $y^2 = x^3 - 3x + 3$.

Structure of elliptic curves

The rational points on elliptic curves form an abelian group!

$$E(\mathbb{Q}) = \{(X, Y) \in \mathbb{Q} \times \mathbb{Q} : Y^2 = X^3 + AX^2 + BX + C\} \cup \{\mathcal{O}\}$$

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r \quad \text{(Mordell, 1922)}$$

They play crucial roles in modern number theory.

The classification of $E(\mathbb{Q})_{\text{tors}}$ (Mazur, 1977)

The group $E(\mathbb{Q})$ contains at most 16 points of finite order.

The rank of elliptic curves : how large ?

There are conjectures on the rank r of elliptic curves

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$$

Current Record : There is an elliptic curve with rank either 28 or 29 (Elkies), and 28 subject to GRH.

Siegel's Theorem

Moreover, we have $\#E(\mathbb{Z}) < \infty$.

Therefore, there is no infinite Diophantine m-tuples.

Similarly,

Generalized Diophantine m-tuples

Fix a natural number $k \geq 2$. A set of natural numbers $S = \{a_1, a_2, \ldots, a_m\}$ is said to satisfy property $D_k(n)$ if $a_i a_j + n$ is a k-th power for all $1 \leq i < j \leq m$.

We analogously define the following quantity for each n,

$$M_k(n) = \sup\{|S| : S \text{ satisfies property } D_k(n)\}$$
$$M_k(n; L) = \sup\{|S \cap [n^L, \infty)| : S \text{ satisfies property } D_k(n)\}$$

For $k \geq 3$ and $m \geq 3$, the theorem of Faltings implies that a superelliptic curve of the form

$$y^k = (a_1x + n)(a_2x + n)(a_3x + n)(a_4x + n) \cdots (a_mx + n)$$

has only finitely many rational points, and hence finitely many integral points. Therefore, a set S satisfying property $D_k(n)$ must be finite.

We produce sharper bounds on $M_k(n)$ under the Paley graph conjecture, namely,

Paley graph conjecture

Let $\epsilon > 0$, $S, T \subseteq \mathbb{F}_p$ for an odd prime p with $|S|, |T| > p^{\epsilon}$, and χ be any non-trivial multiplicative character modulo p. Then, there is $\delta = \delta(\epsilon)$ for which the inequality

$$\left| \sum_{a \in S,\, b \in T} \chi(a+b) \right| \leq p^{-\delta} |S||T|$$

holds for primes p larger than some constant $C(\epsilon)$.

The conjecture is known for the case $|S| > p^{1/2+\epsilon}$ and $|T| > p^{\epsilon}$.

Theorem (Dixit - K. - Murty)

Let $k \geq 3$ be a positive integer. Then, the following holds as $n \to \infty$.

(a) For $L \geq 3$,

$$M_k(n, L) \ll 1,$$

where the implied constant depends on k and L, but is independent of n.

(b) Unconditionally,

$$M_k(n) \ll_k \log n.$$

(c) Assuming the Paley graph conjecture, for any $\epsilon > 0$,

$$M_k(n) \ll_{k,\epsilon} (\log n)^{\epsilon}.$$

Over finite fields ?

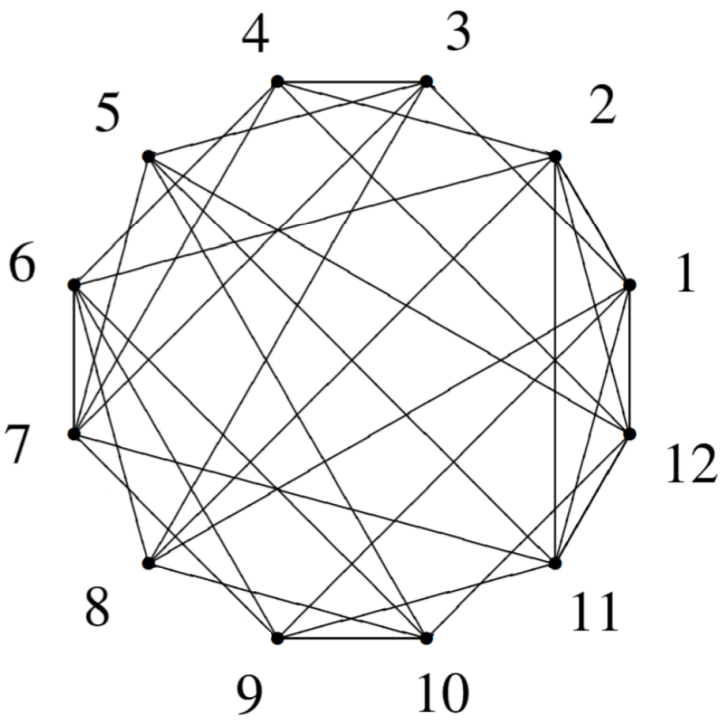
Finite fields are important to test whether there is an integer solution. When $F = \mathbb{F}_q$, Diophantine tuples can be studied using graphs.

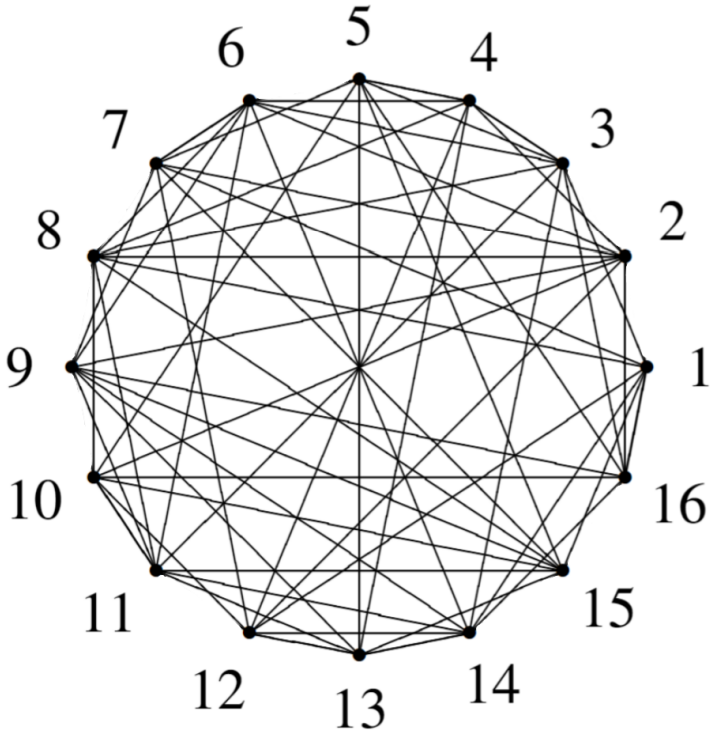
Diophantine graph D_q

The Diophantine graph D_q is the graph whose vertex set is $\mathbb{F}_q^*$, and two vertices x and y are adjacent if and only if $xy + 1$ is a square in $\mathbb{F}_q$.

In particular, the clique number of D_q gives the largest length of Diophantine tuples over $\mathbb{F}_q$.

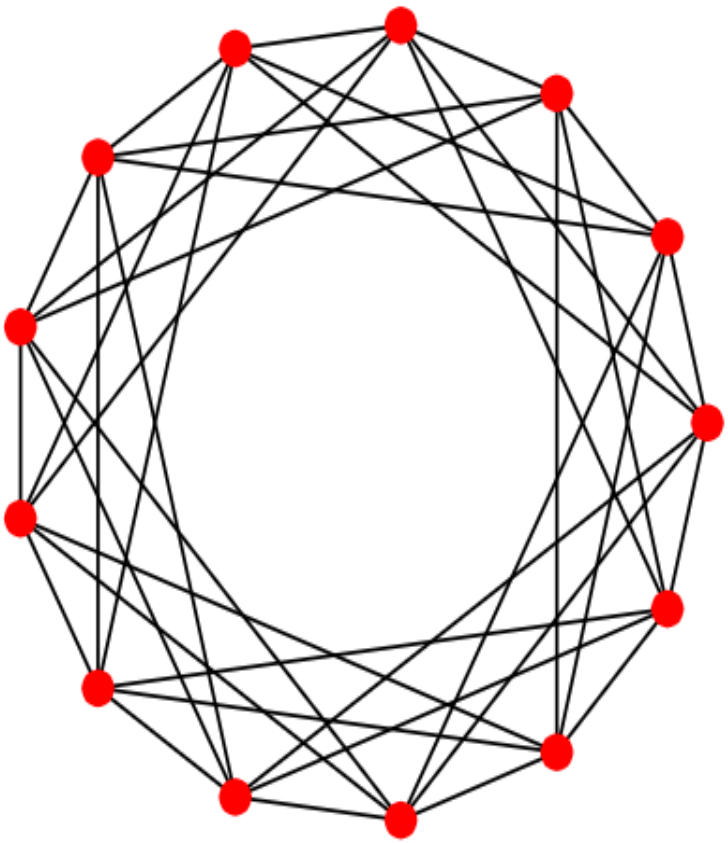
D_{13} and D_{17}

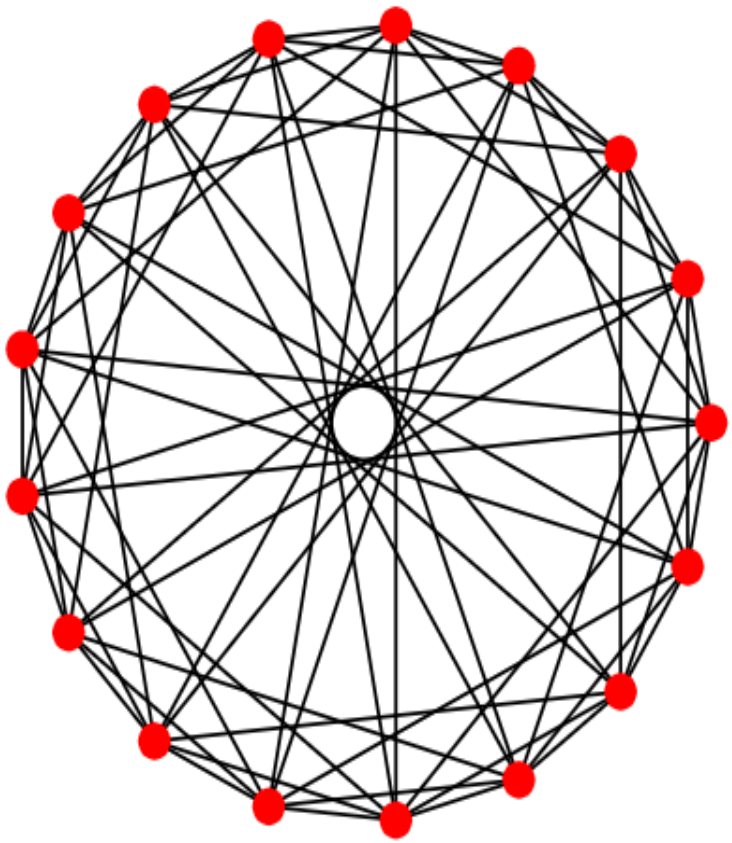




They share many similar properties with Paley graphs! Paley graphs have vertices $\mathbb{F}_q$ and edges (a, b) iff $a - b \in (\mathbb{F}_q^*)^2$

P_{13} and P_{17}





Theorem (K. - Yip - Yoo)

The degrees of vertices of D_q are given as follows.

(1) If $q \equiv 1 \pmod 4$, there are $(q-1)/2$ vertices of degree $(q-1)/2$, and $(q-1)/2$ vertices of degree $(q-3)/2$, with

$$|E(D_q)| = \frac{q^2 - 3q + 2}{4}.$$

(2) If $q \equiv 3 \pmod 4$, there are $(q+1)/2$ vertices of degree $(q-1)/2$, and $(q-3)/2$ vertices of degree $(q-3)/2$

$$|E(D_q)| = \frac{q^2 - 3q + 4}{4}.$$

This implies that, for any prime power q, the graph D_q is almost-regular with diameter 2, and hence connected.

Moreover, we obtained a nontrivial lower bound on the clique number of D_q.

Theorem (K. - Yip - Yoo)

If $q \equiv 1 \pmod 4$, we have

$$\omega(D_q) \geq \frac{p}{p-1}\left\{\frac{\frac{1}{2}\log q - 2\log\log q}{\log 2} + 1\right\}.$$

Furthermore, we expect to improve the lower bound (à la Alon and Solymosi) to

Work in progress (K. - Yip - Yoo)

$\max\{\omega(D_q), \omega(\overline{D_q})\} \geq \log_{3.1} q$.

The conjectural bound is $\omega(D_q) \geq \log_2 q$.

q	$\omega(P_q)$	$\omega(\overline{D_q})$	$\omega(D_q)$	q	$\omega(P_q)$	$\omega(\overline{D_q})$	$\omega(D_q)$	q	$\omega(P_q)$	$\omega(\overline{D_q})$	$\omega(D_q)$
3	*	*	*	83	*	7	8	199	*	9	9
5	2	2	2	89	5	7	8	211	*	9	9
7	*	2	3	97	6	7	8	223	7	10	10
9	3	3	3	101	5	8	8	227	*	10	10
11	*	3	4	103	*	7	8	229	9	10	10
13	3	4	4	107	*	8	8	233	7	10	10
17	3	4	4	109	6	8	8	239	*	10	10
19	*	4	4	113	7	8	8	241	7	10	10
23	*	4	5	121	11	9	10	243	*	11	12
25	5	5	5	125	7	8	8	251	*	10	11
27	*	6	5	127	*	8	8	257	7	10	10
29	4	5	5	131	*	9	9	263	*	11	11
31	*	5	5	137	7	9	9	269	8	10	10
37	4	5	6	139	*	8	9	271	*	10	10
41	5	6	6	149	7	9	9	277	8	10	10
43	*	6	6	151	*	9	9	281	7	10	10
47	*	6	6	157	7	9	9	283	*	10	11
49	7	6	7	163	*	9	9	289	17	11	16
53	5	6	6	167	*	9	9	293	8	10	11
59	*	7	7	169	13	9	12	307	*	11	11
61	5	6	7	173	8	9	9	311	*	11	11
67	*	7	7	179	*	9	9	313	8	11	11
71	*	8	7	181	7	9	10	317	9	11	11
73	5	7	7	191	*	9	9	331	*	11	11
79	*	7	7	193	7	9	9	337	9	11	11
81	9	7	8	197	8	9	10	343	*	11	11

TABLE 3.1. Clique numbers for the Paley graph P_q, the Diophantine graph D_q, and the complement the Diophantine graph $\overline{D_q}$ up to $q = 343$

Thank you !