Incidence bounds over rational points

József Solymosi
Dept. of Mathematics
University of British Columbia, Vancouver

Notes

Jarnik's Theorem

For any curve C, $N(C)$ and $l(C)$ denote its number of integer points and its length respectively.

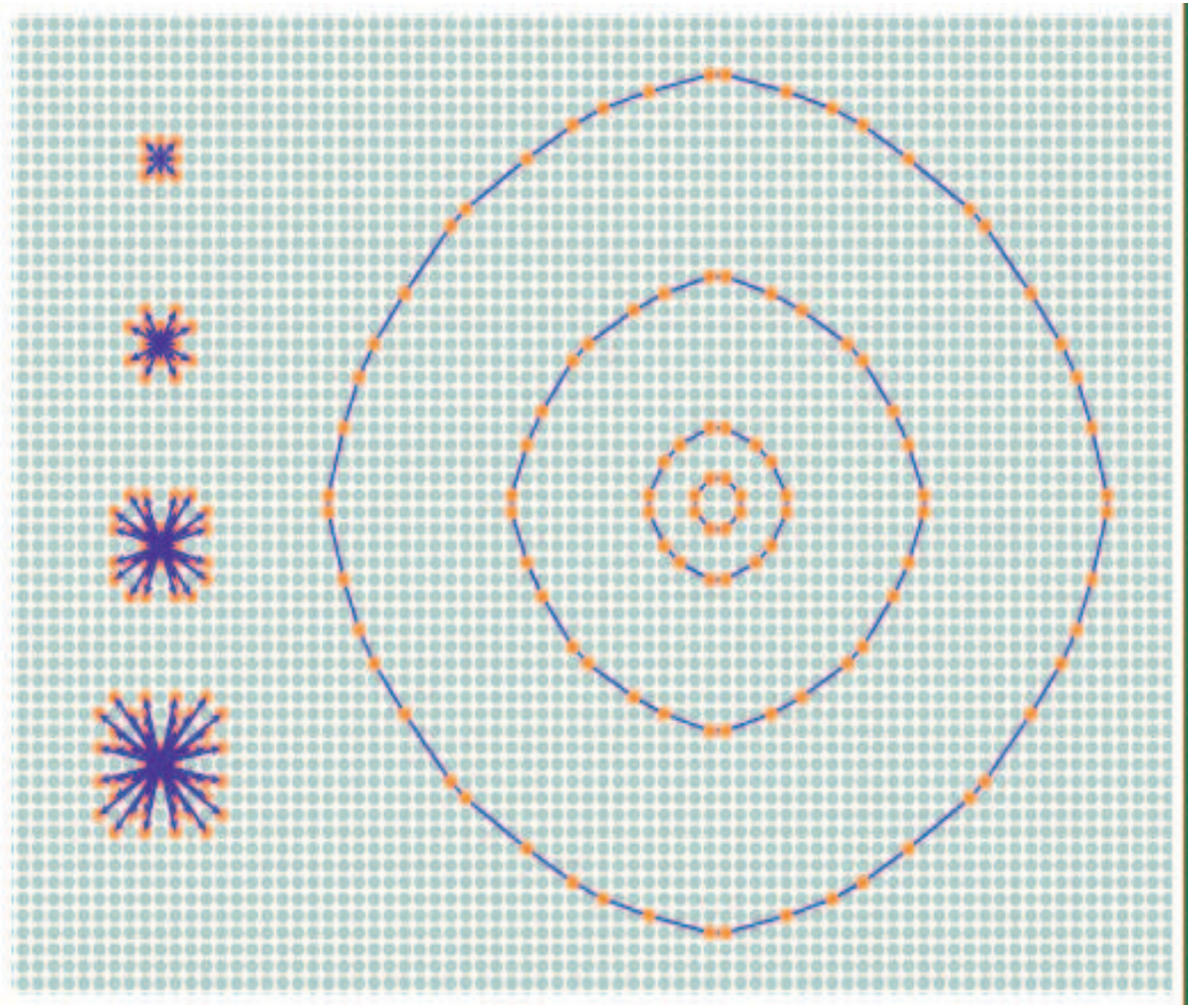
Theorem (Jarnik's Theorem (1926))

For any strictly convex curve, Γ,

$$N(\Gamma) \ll l(\Gamma)^{2/3}.$$

On the other hand, Jarnik constructed a family of strictly convex curves Γ_0, with $l(\Gamma_0)$ tending to infinity, such that

$$N(\Gamma_0) \asymp l(\Gamma_0)^{2/3}.$$



Grekos refined Jarnik's result for C^2 curves. (1988)

$$N(\Gamma) \ll l(\Gamma) r(\Gamma)^{-1/3},$$

where $r(\Gamma)$ denotes the infimum of the radii of curvature of the curve.

It is conjectured by Schmidt (1985) that if Γ is C^3 then

$$N(\Gamma) \ll l(\Gamma)^{1/2+\varepsilon}.$$

Contributions to this problem were made by Swinnerton-Dyer (1974), Schmidt, Bombieri and Pila (1989), and Pila (1991). Plagne gave a uniform version of Jarnik's theorem.

Theorem (Plagne (1999))

Let f be any function tending to infinity. Then there exist a strictly convex curve C and a strictly increasing sequence of integers $\{q_n\}_{n\geq 0}$ such that for each n one has

$$\left| C \bigcap \left(\frac{1}{q}\mathbb{Z} \right)^2 \right| \gg \frac{q_n^{2/3}}{f(q_n)}.$$

(Valtr has also defined a curve with similar property.)

A result of Elekes and Rónyai (1999)

Theorem

For every C and d there is an $n_0 = n_0(C, d)$ such that for any degree d polynomial, F, if $|X| = |Y| \geq n_0$ and the domain of F on X and Y is small, $|F(X, Y)| \leq C|X|$, then

$$F(x, y) = f(g(x) + h(y)),$$

or

$$F(x, y) = f(g(x)h(y)).$$

The main conjecture

Conjecture

For every C and d there is an $n_0 = n_0(C, d)$ such that for any degree d polynomial, F, if $|X| = |Y| \geq n_0, X, Y \subset \mathbb{Q}$, and $|F(X, Y)| \leq C|X|$, then

$$F(x, y) = f(ax + by + c),$$

or

$$F(x, y) = f((x + a)^n (y + b)^m).$$

Why should be the conjecture true?

- We can prove the Conjecture (and more) if F has degree 2.
- Conjecture would follow from the Bombieri-Lang conjecture.
- We can prove the conclusion of Conjecture if there are infinite sequences of sets

$$X_1 \subset X_2 \subset X_3 \subset \ldots X_i \subset \ldots \subset \mathbb{Q}$$

$$Y_1 \subset Y_2 \subset Y_3 \subset \ldots Y_i \subset \ldots \subset \mathbb{Q}$$

such that $|X_i| = |Y_i|$ and $|F(X_i, Y_i)| \leq C|X_i|$.

A curve C of genus at least 2 defined over a function field L has only finitely many L rational points, unless it is isotrivial. Similarly, a curve of genus at least 2 defined over a number field F has a finite set of F-rational points. These well-known facts are celebrated theorems of Y. Manin and G. Faltings, originally conjectured by L. J. Mordell and S. Lang.

We won't define here the genus exactly. However it is good to know that hyperelliptic curves of genus g, defined over the rationals, can be put in the form

$$C : y^2 = f(x)$$

where $f(x)$ is a polynomial with integer coefficients of degree $2g + 2$ or $2g + 1$, which has no repeated roots.

Uniform Mordell Conjecture for number fields

Caporasso, Harris, and Mazur proved (1997) that the Bombieri-Lang conjecture would imply the following.

Conjecture (Uniform Mordell Conjecture)

Fix $g \geq 2$ and a number field F; there exists a number $B_g(F)$ such that any curve of genus g defined over F has at most $B_g(F)$ rational points over F.

Corollaries of the Uniform Mordell Conjecture

Corollary

For every polynomial, $f(x)$, having degree ≥ 2 there is a number, k, such that $y = f(x)$ has no integer points forming a k-term arithmetic progression.

Corollary

For every polynomial, $f(x)$, having at least two distinct roots there is a number, k, such that $y = f(x)$ has no integer points forming a k-term geometric progression.

Theorem

If the Bombieri-Lang conjecture is true then for every C and d there is an $n_0 = n_0(C, d)$ such that for any degree d polynomial, F, if $|X| = |Y| \geq n_0, X, Y \subset \mathbb{Q}$, and $|F(X, Y)| \leq C|X|$, then

$$F(x, y) = f(ax + by + c),$$

or

$$F(x, y) = f((x + a)^n (y + b)^m).$$

The key elements of the proof:

- From the Elekes-Rónyai Theorem we know that

$$F(x, y) = f(g(x) + h(y)),$$

  or

$$F(x, y) = f(g(x)h(y)).$$

- If $|g(X) + h(Y)|$ is small then $|g(X) + g(X)|$ is also small. (Plünecke-Ruzsa type inequality)
- By Freiman's theorem $g(X)$ is a dense subset of a low dimensional generalized arithmetic progression.
- Szemerédi's theorem implies that $g(X)$ has long arithmetic progressions.

Repeat the argument for the product case.

Theorem

If $F(x, y)$ is a quadratic polynomial, $|X| = |Y| \geq n_0, X, Y \subset \mathbb{Q}$, and $|F(X, Y)| \leq (\log |X|)^{\delta}|X|$, then

$$F(x, y) = f(ax + by + c),$$

or

$$F(x, y) = c(x + a)(y + b) + d.$$

The Elekes-Rónyai result is not enough here. There is a stronger result of Elekes and Szabó.

Elekes-Szabó

Theorem (Elekes-Szabó (2007+))

Given a surface, S, by the $F(x, y, z) = 0$ equation. (F is a polynomial of three variables) If

$$|S \bigcap X \times Y \times Z| \geq n^{2-\delta}$$

for some $|X| = |Y| = |Z| = n \geq n_0$ sets then

$$F(x, y, z) = f(g(x) + h(y) + t(z)).$$

Here $f, g, h,$ and t are analytical functions.

Theorem

For any degree d polynomial, F, if there are infinite sequences

$$X_1 \subset X_2 \subset X_3 \subset \ldots X_i \subset \ldots \subset \mathbb{Q}$$

$$Y_1 \subset Y_2 \subset Y_3 \subset \ldots Y_i \subset \ldots \subset \mathbb{Q}$$

such that $|X_i| = |Y_i|$ *and* $|F(X_i, Y_i)| \leq C|X_i|$, *then*

$$F(x, y) = f(ax + by + c),$$

or

$$F(x, y) = f((x + a)^n (y + b)^m).$$

Freiman's Theorem

For the proof we need (again) the following lemma.

Lemma (Freiman's Dimension Lemma)

If $A, B \subset \mathbb{C}$,

$$|A * B| < KN$$

and

$$|A| = |B| = N,$$

then A and B are subsets of a multiplicative subgroup of rank $r = r(K)$.

If

$$F(x, y) = f(g(x)h(y)),$$

then all $g(X_i)$-s are contained in a multiplicative subgroup of rank $r = r(C)$. But it contradicts to the following result.

Theorem (Shorey and Tijdeman (1976))

Let $f(x)$ be a polynomial with integer coefficients and at least two distinct roots. Then for every k there is an $x_0 = x_0(k)$ such that if $x \geq x_0$ then either $f(x)$ has at least k distinct prime divisors or the largest prime divisor of $f(x)$ is larger than k.