Points on polynomial curves in small boxes modulo an integer

1st FGC-IPM Joint Number Theory Meeting

Ali Mohammadi
Joint work with Bryce Kerr

Institute for Research in Fundamental Sciences (IPM)

15 March 2021

Objective

Let q denote an integer and $f \in \mathbb{Z}_q[X]$ a polynomial of degree $d = 3$. Let $\mathcal{B}$ denote a box of side length $H \leq q$. Namely,

$$\mathcal{B} = [R, R + H] \times [S, S + H] \subset \mathbb{Z} \times \mathbb{Z}.$$

Objective

Let q denote an integer and $f \in \mathbb{Z}_q[X]$ a polynomial of degree $d = 3$. Let $\mathcal{B}$ denote a box of side length $H \leq q$. Namely,

$$\mathcal{B} = [R, R + H] \times [S, S + H] \subset \mathbb{Z} \times \mathbb{Z}.$$

We wish to bound the number of solutions to the equation

$$y^2 \equiv f(x) \pmod{q},$$

with $(x, y) \in \mathcal{B}$.

Objective

Let q denote an integer and $f \in \mathbb{Z}_q[X]$ a polynomial of degree $d = 3$. Let $\mathcal{B}$ denote a box of side length $H \leq q$. Namely,

$$\mathcal{B} = [R, R + H] \times [S, S + H] \subset \mathbb{Z} \times \mathbb{Z}.$$

We wish to bound the number of solutions to the equation

$$y^2 \equiv f(x) \pmod{q},$$

with $(x, y) \in \mathcal{B}$.
The methods that we will describe will yield results for the more general type of equation

$$g(y) \equiv f(x) \pmod{q},$$

with $(x, y) \in \mathcal{B}$, assuming $\deg(g)$ and $\deg(f)$ are coprime.

A related result

Theorem (Bombieri and Pila 1989)

Let $\mathcal{C}$ be an absolutely irreducible plane curve of degree $d \geq 2$ and suppose $H \geq e^{d^6}$. The number of integral points on $\mathcal{C}$ and inside a square $[0, H] \times [0, H]$ is bounded by

$$O\left(H^{1/d+o(1)}\right).$$

A related result

Theorem (Bombieri and Pila 1989)

Let $\mathcal{C}$ be an absolutely irreducible plane curve of degree $d \geq 2$ and suppose $H \geq e^{d^6}$. The number of integral points on $\mathcal{C}$ and inside a square $[0, H] \times [0, H]$ is bounded by

$$O\left(H^{1/d+o(1)}\right).$$

Remark

This estimate is essentially best possible. Consider for example

$$f(x, y) = x^d - y.$$

Then, there are $\approx H^{1/d}$ solutions $(x, y) = (m, m^d)$ with $m \leq H^{1/d}$.

Remark

We, generally, have a good understanding of this problem when H is "large". For instance, for a prime p, it is known from the Weil bounds that if $y^2 - f(x)$ is absolutely irreducible, then

$$|\{(x, y) \in \mathcal{B} \ : \ y^2 \equiv f(x) \pmod{p}\}| = \frac{H^2}{p} + O(p^{1/2}(\log p)^2).$$

Known results

Remark

We, generally, have a good understanding of this problem when H is "large". For instance, for a prime p, it is known from the Weil bounds that if $y^2 - f(x)$ is absolutely irreducible, then

$$|\{(x, y) \in \mathcal{B} \ : \ y^2 \equiv f(x) \pmod{p}\}| = \frac{H^2}{p} + O(p^{1/2}(\log p)^2).$$

Noting that the trivial upper-bound is $O(H)$, this result is trivial when $H = O(p^{1/2}(\log p)^2)$.

Known results

Theorem (Chang, Cilleruelo, Garaev, Hernandez, Shparlinski and Zumalacarregui 2011)

Let p be a prime, $f \in \mathbb{Z}_p[X]$ of degree $d = 3$ and $\mathcal{B}$ a square of side length H. Then we have

$$|\{(x,y) \in \mathcal{B} \ : \ y^2 \equiv f(x) \pmod{p}\}| \ll \begin{cases} H^{1/3+o(1)}, & \text{if} \quad H < p^{1/8}, \\ \left(\frac{H^4}{p}\right)^{1/6} H^{1+o(1)}, & \text{if} \quad p^{1/8} \le H < p^{5/23}, \\ \left(\frac{H^3}{p}\right)^{1/16} H^{1+o(1)}, & \text{if} \quad p^{5/23} \le H < p^{1/3}. \end{cases}$$

Theorem (Kerr and M. 2020)

Let q be an arbitrary integer, $f \in \mathbb{Z}_q[X]$ of degree $d = 3$, such that its leading coefficient is coprime with q and let $\mathcal{B}$ denote a square of side length H. Then we have

$$|\{(x, y) \in \mathcal{B} \ : \ y^2 \equiv f(x) \pmod{q}\}| \ll \frac{H^{3/2}}{q^{1/6}} + H^{1/3+o(1)}.$$

In particular if $H \leq q^{1/7}$ then

$$|\{(x, y) \in \mathcal{B} \ : \ y^2 \equiv f(x) \pmod{q}\}| \leq H^{1/3+o(1)}.$$

Theorem (Kerr and M. 2020)

Let q be an arbitrary integer, $f \in \mathbb{Z}_q[X]$ of degree $d = 3$, such that its leading coefficient is coprime with q and let $\mathcal{B}$ denote a square of side length H. Then we have

$$|\{(x, y) \in \mathcal{B} \ : \ y^2 \equiv f(x) \pmod{q}\}| \ll \frac{H^{3/2}}{q^{1/6}} + H^{1/3+o(1)}.$$

In particular if $H \leq q^{1/7}$ then

$$|\{(x, y) \in \mathcal{B} \ : \ y^2 \equiv f(x) \pmod{q}\}| \leq H^{1/3+o(1)}.$$

This improves the result of Chang, Cilleruelo, Garaev, Hernandez, Shparlinski and Zumalacarregui for $p^{1/8} \leq H \leq p^{1/3}$ and matches it for $H < p^{1/8}$.

Theorem (Kerr and M. 2020)

Let q be an arbitrary integer, $f \in \mathbb{Z}_q[X]$ a polynomial of degree $d \geq 2$ with leading coefficient a_d satisfying $(a_d, q) = 1$ and suppose $\mathcal{B}$ is a cube of side length H. Then we have

$$|\{(x, y) \in \mathcal{B} \ : \ y \equiv f(x) \pmod{q}\}| \leq \frac{H^{1+2/d(d+1)+o(1)}}{q^{2/d(d+1)}} + H^{1/d+o(1)}.$$

In particular if

$$H \leq q^{2/(d^2+1)},$$

then

$$|\{(x, y) \in \mathcal{B} \ : \ y \equiv f(x) \pmod{q}\}| \leq H^{1/d+o(1)}.$$

Initiating the proof (shift of variables)

Fix a solution $(x_0, y_0) \in \mathcal{B}$ of the equation

$$y^2 \equiv f(x) \pmod{q}.$$

Initiating the proof (shift of variables)

Fix a solution $(x_0, y_0) \in \mathcal{B}$ of the equation

$$y^2 \equiv f(x) \pmod{q}.$$

By making the shift of variables $(x, y) \mapsto (x - x_0, y - y_0)$, it is sufficient to bound the number of solutions to

$$y^2 - c_0 y \equiv a_3 x^3 + a_2 x^2 + a_1 x \pmod{q}, \quad |x|, |y| \leq H. \qquad (1)$$

Initiating the proof (shift of variables)

Fix a solution $(x_0, y_0) \in \mathcal{B}$ of the equation

$$y^2 \equiv f(x) \pmod{q}.$$

By making the shift of variables $(x, y) \mapsto (x - x_0, y - y_0)$, it is sufficient to bound the number of solutions to

$$y^2 - c_0 y \equiv a_3 x^3 + a_2 x^2 + a_1 x \pmod{q}, \quad |x|, |y| \leq H. \qquad (1)$$

Let $\mathcal{X} = \{x : (x, y) \text{ satisfies } (1)\}$. Then it suffices to bound $|\mathcal{X}|$ since the number of solutions to (1) is bounded by $2|\mathcal{X}|$.

A quick sketch

Let us consider the linear equation $y_2 - c_0 y_1 \equiv a_3 x_3 + a_2 x_2 + a_1 x_1 \pmod{q}$, which defines a lattice in $\mathbb{Z}^5$.

A quick sketch

Let us consider the linear equation $y_2 - c_0 y_1 \equiv a_3 x_3 + a_2 x_2 + a_1 x_1 \pmod{q}$, which defines a lattice in $\mathbb{Z}^5$. There are two main steps:

A quick sketch

Let us consider the linear equation $y_2 - c_0 y_1 \equiv a_3 x_3 + a_2 x_2 + a_1 x_1 \pmod{q}$, which defines a lattice in $\mathbb{Z}^5$. There are two main steps:

1. We show this lattice has a "large" intersection with an appropriately chosen convex body, in terms of the number of solutions to our original polynomial equation.
   This uses results on the Vinogradov's mean value theorem.

A quick sketch

Let us consider the linear equation $y_2 - c_0 y_1 \equiv a_3 x_3 + a_2 x_2 + a_1 x_1 \pmod{q}$, which defines a lattice in $\mathbb{Z}^5$. There are two main steps:

1. We show this lattice has a "large" intersection with an appropriately chosen convex body, in terms of the number of solutions to our original polynomial equation.
   This uses results on the Vinogradov's mean value theorem.
2. Based on the relative geometry of the lattice and the convex body we consider two cases:

A quick sketch

Let us consider the linear equation $y_2 - c_0 y_1 \equiv a_3 x_3 + a_2 x_2 + a_1 x_1 \pmod{q}$, which defines a lattice in $\mathbb{Z}^5$. There are two main steps:

1. We show this lattice has a "large" intersection with an appropriately chosen convex body, in terms of the number of solutions to our original polynomial equation.
   This uses results on the Vinogradov's mean value theorem.
2. Based on the relative geometry of the lattice and the convex body we consider two cases:
   1. If the lattice fills the body "tightly", we can bound from above their intersection and be done.
      This uses Minkowski's second theorem.

A quick sketch

Let us consider the linear equation $y_2 - c_0 y_1 \equiv a_3 x_3 + a_2 x_2 + a_1 x_1 \pmod{q}$, which defines a lattice in $\mathbb{Z}^5$. There are two main steps:

1. We show this lattice has a "large" intersection with an appropriately chosen convex body, in terms of the number of solutions to our original polynomial equation.
   This uses results on the Vinogradov's mean value theorem.
2. Based on the relative geometry of the lattice and the convex body we consider two cases:
   1. If the lattice fills the body "tightly", we can bound from above their intersection and be done.
      This uses Minkowski's second theorem.
   2. If not, we find a vector in the intersection of the duals of our lattice and body, which will help us "lift" the equation to $\mathbb{Z}$, where we may use the Bombieri-Pila theorem.
      This uses a transference result of Banaszczyk.

Definition (Lattices)

A lattice Γ in $\mathbb{R}^n$ is any additive subgroup of the Euclidean space $\mathbb{R}^n$ which is discrete. We define the rank k of Γ to be the dimension of the linear space spanned by the elements of Γ, thus $0 \leq k \leq n$. If $k = n$, we say Γ has full rank.

Definition (Lattices)

A lattice Γ in $\mathbb{R}^n$ is any additive subgroup of the Euclidean space $\mathbb{R}^n$ which is discrete. We define the rank k of Γ to be the dimension of the linear space spanned by the elements of Γ, thus $0 \leq k \leq n$. If $k = n$, we say Γ has full rank.

Definition (Convex bodies)

Recall that a set, $A \subset \mathbb{R}^n$, is convex if we have $(1-\theta)x + \theta y \in A$ whenever $x, y \in A$ and $0 \leq \theta \leq 1$. We call a set, $A \subset \mathbb{R}^n$, a convex body if it is convex, open, non-empty and bounded. Furthermore, we call a convex body A symmetric if $A = -A$.

Dual lattice

Definition (Dual lattice)

We define the dual lattice Γ^* of Γ by

$$\Gamma^* = \{y \in \mathbb{R}^n \ : \ \langle y, z\rangle \in \mathbb{Z} \ \text{ for all } z \in \Gamma\},$$

where $\langle ., . \rangle$ denotes the Euclidean inner product.

Dual lattice

Definition (Dual lattice)

We define the dual lattice Γ^* of Γ by

$$\Gamma^* = \{y \in \mathbb{R}^n \ : \ \langle y, z\rangle \in \mathbb{Z} \ \text{ for all } z \in \Gamma\},$$

where $\langle ., . \rangle$ denotes the Euclidean inner product.

Examples:

- $(\mathbb{Z}^n)^* = \mathbb{Z}^n$.

Dual lattice

Definition (Dual lattice)

We define the dual lattice Γ^* of Γ by

$$\Gamma^* = \{y \in \mathbb{R}^n \ : \ \langle y, z\rangle \in \mathbb{Z} \ \text{ for all } z \in \Gamma\},$$

where $\langle ., . \rangle$ denotes the Euclidean inner product.

Examples:

- $(\mathbb{Z}^n)^* = \mathbb{Z}^n$.
- For every real $m > 0$ and every lattice Γ, we have $(m\Gamma)^* = m^{-1}\Gamma^*$.

The lattice $2\mathbb{Z}^2$ and its dual lattice $2^{-1}\mathbb{Z}^2$

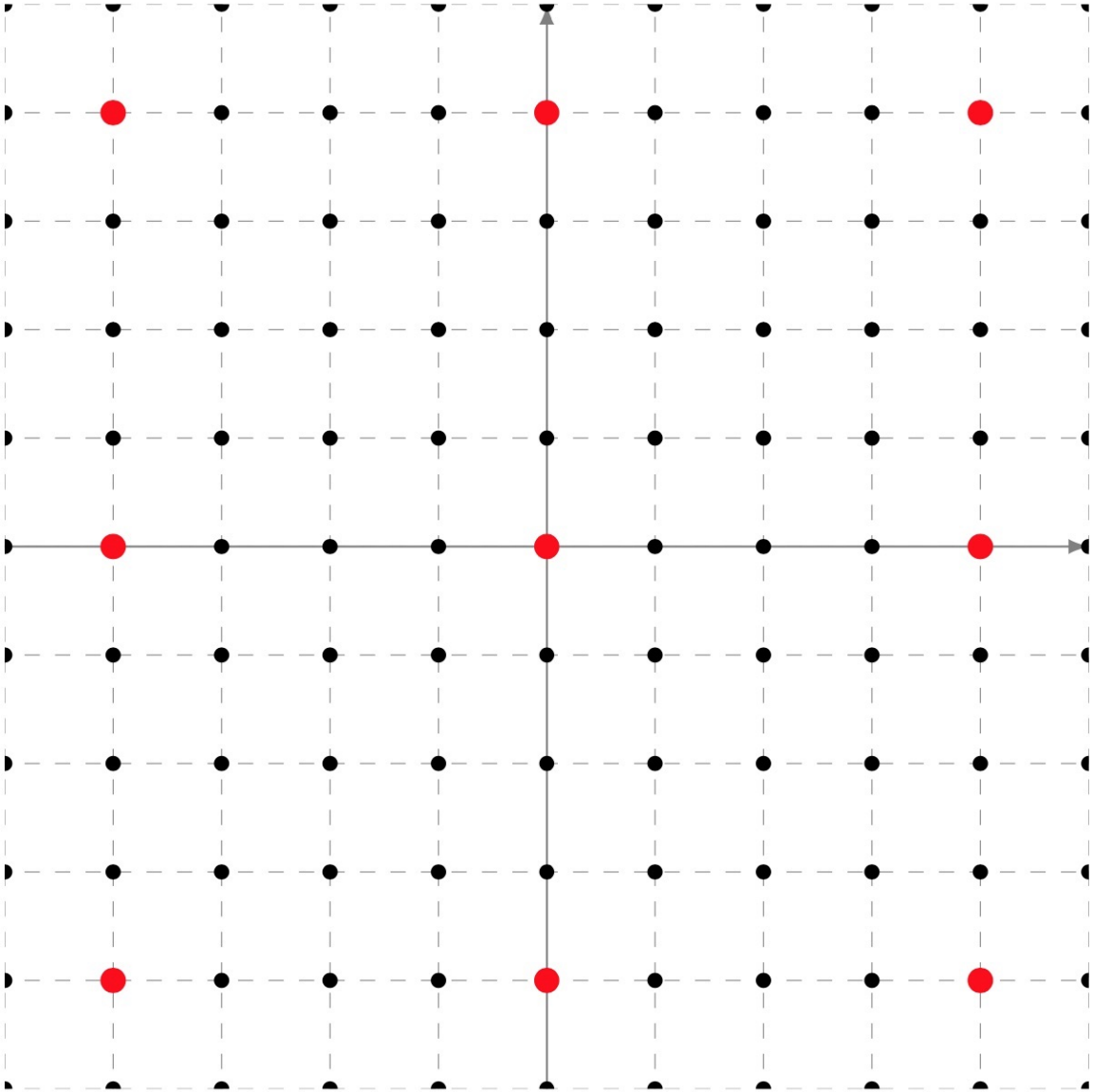

Image Credit: Luca Notarnicola

Dual body

Definition (Dual body)

The dual body D^* of D by

$$D^* = \{y \in \mathbb{R}^n \ : \ \langle y, z\rangle \leq 1 \ \text{ for all } z \in D\},$$

where $\langle ., . \rangle$ denotes the Euclidean inner product.

Dual body

Definition (Dual body)

The dual body D^* of D by

$$D^* = \{y \in \mathbb{R}^n \ : \ \langle y, z \rangle \leq 1 \ \text{ for all } z \in D\},$$

where $\langle ., . \rangle$ denotes the Euclidean inner product.

Examples:

- The Euclidean unit ball $\{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_1^2 + \cdots + x_n^2 \leq 1\}$ is self-dual.

Dual body

Definition (Dual body)

The dual body D^* of D by

$$D^* = \{y \in \mathbb{R}^n \ : \ \langle y, z\rangle \leq 1 \ \text{ for all } z \in D\},$$

where $\langle ., . \rangle$ denotes the Euclidean inner product.

Examples:

- The Euclidean unit ball $\{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_1^2 + \cdots + x_n^2 \leq 1\}$ is self-dual.
- The dual of $[-1, 1]^2$ is the polytope $|x| + |y| \leq 1$.

Dual body

Definition (Dual body)

The dual body D^* of D by

$$D^* = \{y \in \mathbb{R}^n \ : \ \langle y, z\rangle \leq 1 \ \text{ for all } z \in D\},$$

where $\langle ., . \rangle$ denotes the Euclidean inner product.

Examples:

- The Euclidean unit ball $\{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_1^2 + \cdots + x_n^2 \leq 1\}$ is self-dual.
- The dual of $[-1, 1]^2$ is the polytope $|x| + |y| \leq 1$.
- The dual of $\Pi_{i=1}^n [-H_i, H_i]$, with $H_i > 0$ is $\{(x_1, \ldots, x_n) \in \mathbb{R}^n : |x_1|H_1 + \cdots + |x_n|H_n \leq 1\}$

Successive minima

Definition (Successive minima)

Given a lattice $\Gamma \subset \mathbb{R}^n$ and a symmetric convex body $D \subset \mathbb{R}^n$ we define the i-th successive minimum of Γ with respect to D by

$$\lambda_i = \inf\{\lambda : \Gamma \cap \lambda D \text{ contains } i \text{ linearly independent points}\}.$$

Successive minima

Definition (Successive minima)

Given a lattice $\Gamma \subset \mathbb{R}^n$ and a symmetric convex body $D \subset \mathbb{R}^n$ we define the i-th successive minimum of Γ with respect to D by

$$\lambda_i = \inf\{\lambda : \Gamma \cap \lambda D \text{ contains } i \text{ linearly independent points}\}.$$

- Certainly, always $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$.

Successive minima

Definition (Successive minima)

Given a lattice $\Gamma \subset \mathbb{R}^n$ and a symmetric convex body $D \subset \mathbb{R}^n$ we define the i-th successive minimum of Γ with respect to D by

$$\lambda_i = \inf\{\lambda : \Gamma \cap \lambda D \text{ contains } i \text{ linearly independent points}\}.$$

- Certainly, always $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$.
- These may be viewed as a measure of how "stretched" a lattice is w.r.t. a body.

Successive minima

Definition (Successive minima)

Given a lattice $\Gamma \subset \mathbb{R}^n$ and a symmetric convex body $D \subset \mathbb{R}^n$ we define the i-th successive minimum of Γ with respect to D by

$$\lambda_i = \inf\{\lambda : \Gamma \cap \lambda D \text{ contains } i \text{ linearly independent points}\}.$$

- Certainly, always $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$.
- These may be viewed as a measure of how "stretched" a lattice is w.r.t. a body.
- When $\Gamma = \mathbb{Z}^n$ and D is the Euclidean ball, we have $\lambda_1 = \cdots = \lambda_n = 1$.

Successive minima w.r.t. a Euclidean ball

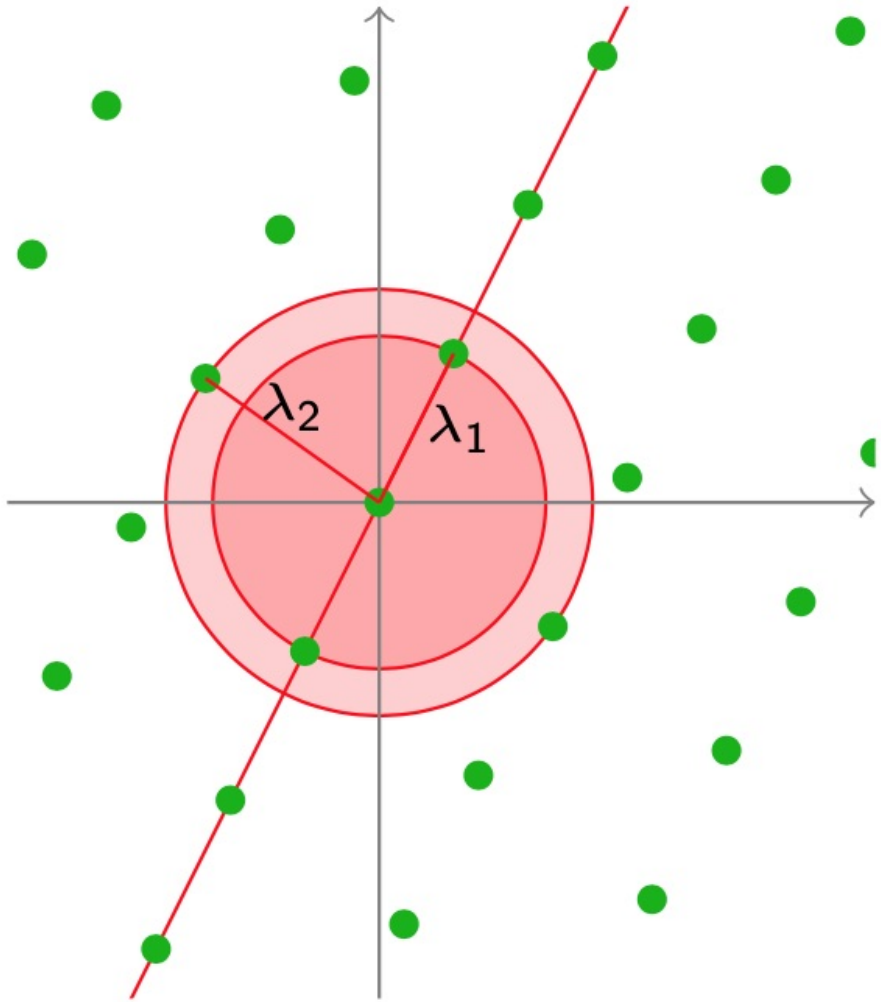

Image credit: Daniele Micciancio

The dichotomy of the size of λ_n

The following is a consequence of Minskowski's second theorem.

Lemma

Let $\Gamma \subset \mathbb{R}^n$ be a lattice, $D \subset \mathbb{R}^n$ a symmetric convex body and let λ_n denote the n-th successive minima of Γ with respect to D. If $\lambda_n \leq 1$, then

$$|\Gamma \cap D| \ll_n \frac{Vol(D)}{|\mathbb{R}^n/\Gamma|}.$$

The dichotomy of the size of λ_n

The following is a consequence of Minskowski's second theorem.

Lemma

Let $\Gamma \subset \mathbb{R}^n$ be a lattice, $D \subset \mathbb{R}^n$ a symmetric convex body and let λ_n denote the n-th successive minima of Γ with respect to D. If $\lambda_n \leq 1$, then

$$|\Gamma \cap D| \ll_n \frac{Vol(D)}{|\mathbb{R}^n/\Gamma|}.$$

The following is a consequence of a transference result of Banaszczyk (1995).

Lemma

Let $\Gamma \subset \mathbb{R}^n$ be a lattice, $D \subset \mathbb{R}^n$ a symmetric convex body and let $\lambda_1, \ldots, \lambda_n$ denote the successive minima of Γ with respect to D. If $\lambda_n \geq 1$, then

$$\lambda_1^* \ll 1.$$

Vinogradov's mean value theorem

Lemma (Bourgain, Demeter and Guth 2016 and Wooley 2018)

Let $\mathcal{X} \subset [1, H]$ be some set. For integers k and s we let $J_{k,s}(\mathcal{X})$ denote the number of solutions to the system of equations

$$x_1^j + \cdots + x_s^j = x_{s+1}^j + \cdots + x_{2s}^j, \quad 1 \leq j \leq k,$$

with variables

$$x_1, \ldots, x_{2s} \in \mathcal{X}.$$

For $s \leq k(k+1)/2$ we have

$$J_{k,s}(\mathcal{X}) \ll |\mathcal{X}|^s H^{o(1)}.$$

Vinogradov's mean value theorem

Corollary

The number of solutions to the system of diophantine equations

$$x_1^j + \cdots + x_6^j = x_7^j + \cdots + x_{12}^j, \quad 1 \leq j \leq 3,$$

with $x_i \in \mathcal{X} \subset [-H, H]$ *is at most* $|\mathcal{X}|^6 H^{o(1)}$.

1st phase of the proof (choosing suitable Γ and D)

Define the intervals

$$I_j = [-6H^j, 6H^j], \qquad j = 1, 2, 3,$$

and consider the set

$$\mathcal{S} \subseteq I_1 \times I_2 \times I_3,$$

of all triples

$$\tilde{x} = (x_1 + \ldots + x_6,\ x_1^2 + \ldots + x_6^2,\ x_1^3 + \ldots + x_6^3), \qquad (2)$$

such that $x_i \in \mathcal{X}$.

1st phase of the proof (choosing suitable Γ and D)

Define the intervals

$$I_j = [-6H^j, 6H^j], \qquad j = 1, 2, 3,$$

and consider the set

$$\mathcal{S} \subseteq I_1 \times I_2 \times I_3,$$

of all triples

$$\tilde{x} = (x_1 + \ldots + x_6,\ x_1^2 + \ldots + x_6^2,\ x_1^3 + \ldots + x_6^3), \qquad (2)$$

such that $x_i \in \mathcal{X}$. For each $\tilde{x}$ we let $I(\tilde{x})$ count the number of distinct solutions to the equation (2) with variables $x_1, \ldots, x_6 \in \mathcal{X}$. Thus

$$\sum_{\tilde{x} \in \mathcal{S}} I(\tilde{x}) = |\mathcal{X}|^6 \quad \text{and} \quad \sum_{\tilde{x} \in \mathcal{S}} I(\tilde{x})^2 \leq H^{o(1)} |\mathcal{X}|^6.$$

1st phase of the proof (choosing suitable Γ and D)

By the Cauchy-Schwarz inequality, we have

$$|\mathcal{X}|^6 = \sum_{\tilde{x}\in\mathcal{S}} I(\tilde{x}) \leq \left(|\mathcal{S}| \sum_{\tilde{x}\in\mathcal{S}} I(\tilde{x})^2 \right)^{1/2},$$

1st phase of the proof (choosing suitable Γ and D)

By the Cauchy-Schwarz inequality, we have

$$|\mathcal{X}|^6 = \sum_{\tilde{x} \in \mathcal{S}} I(\tilde{x}) \leq \left(|\mathcal{S}| \sum_{\tilde{x} \in \mathcal{S}} I(\tilde{x})^2 \right)^{1/2},$$

which implies that

$$|\mathcal{S}| \geq |\mathcal{X}|^6 H^{-o(1)}.$$

1st phase of the proof (choosing suitable Γ and D)

By the Cauchy-Schwarz inequality, we have

$$|\mathcal{X}|^6 = \sum_{\tilde{x} \in \mathcal{S}} I(\tilde{x}) \leq \left(|\mathcal{S}| \sum_{\tilde{x} \in \mathcal{S}} I(\tilde{x})^2 \right)^{1/2},$$

which implies that

$$|\mathcal{S}| \geq |\mathcal{X}|^6 H^{-o(1)}.$$

Hence, there exist at least $|\mathcal{X}|^6 H^{-o(1)}$ triples

$$(x_1, x_2, x_3) \in I_1 \times I_2 \times I_3,$$

such that

$$a_3 x_3 + a_2 x_2 + a_1 x_1 \equiv y_2 - c_0 y_1 \pmod{q},$$

for some $y_2 \in I_2$ and $y_1 \in I_1$.

1st phase of the proof (choosing suitable Γ and D)

In particular, we have that the congruence

$$a_1x_1 + a_2x_2 + a_3x_3 + c_0y_1 + y_2 \equiv 0 \pmod{q},$$
$$(x_1, x_2, x_3, y_1, y_2) \in I_1 \times I_2 \times I_3 \times I_1 \times I_2,$$

has a set of solutions $\mathcal{S}$ with

$$|\mathcal{S}| \geq |\mathcal{X}|^6 H^{-o(1)}.$$

1st phase of the proof (choosing suitable Γ and D)

Thus, defining the lattice

$$\Gamma = \{(x_1, x_2, x_3, y_1, y_2) \in \mathbb{Z}^5 \ : \\ a_1x_1 + a_2x_2 + a_3x_3 + c_0y_1 + y_2 \equiv 0 \pmod{q}\},$$

and the body

$$D = \{(x_1, x_2, x_3, y_1, y_2) \in \mathbb{R}^5 \ : \\ |x_1|, |y_1| \leq 6H, \ |x_2|, |y_2| \leq 6H^2, \ |x_3| \leq 6H^3\},$$

we have

$$|\mathcal{X}|^6 H^{-o(1)} \ll |\Gamma \cap D|.$$

2nd phase of the proof (Case 1: $\lambda_5 \leq 1$)

Suppose $\lambda_5 \leq 1$. Then

$$|\Gamma \cap D| \ll \frac{\mathrm{Vol}(D)}{|\mathbb{R}^5/\Gamma|} \ll \frac{H^9}{q}.$$

2nd phase of the proof (Case 1: $\lambda_5 \leq 1$)

Suppose $\lambda_5 \leq 1$. Then

$$|\Gamma \cap D| \ll \frac{\mathrm{Vol}(D)}{|\mathbb{R}^5/\Gamma|} \ll \frac{H^9}{q}.$$

Recalling the lower bound

$$|\mathcal{X}|^6 H^{-o(1)} \ll |\Gamma \cap D|,$$

we obtain

$$|\mathcal{X}| \leq \frac{H^{3/2+o(1)}}{q^{1/6}}.$$

2nd phase of the proof (Case 2: $\lambda_5 > 1$)

Recall the definitions

$$\Gamma = \{(x_1, x_2, x_3, y_1, y_2) \in \mathbb{Z}^5 \ : \\ a_1x_1 + a_2x_2 + a_3x_3 + c_0y_1 + y_2 \equiv 0 \pmod{q}\}$$

and

$$D = \{(x_1, x_2, x_3, y_1, y_2) \in \mathbb{R}^5 \ : \\ |x_1|, |y_1| \leq 6H, \ |x_2|, |y_2| \leq 6H^2, \ |x_3| \leq 6H^3\}.$$

2nd phase of the proof (Case 2: $\lambda_5 > 1$)

Recall the definitions

$$\Gamma = \{(x_1, x_2, x_3, y_1, y_2) \in \mathbb{Z}^5 \ : \\ a_1x_1 + a_2x_2 + a_3x_3 + c_0y_1 + y_2 \equiv 0 \pmod{q}\}$$

and

$$D = \{(x_1, x_2, x_3, y_1, y_2) \in \mathbb{R}^5 \ : \\ |x_1|, |y_1| \leq 6H, \ |x_2|, |y_2| \leq 6H^2, \ |x_3| \leq 6H^3\}.$$

Then we have

$$\Gamma^* = \frac{1}{q}\{(w_1, w_2, w_3, z_1, z_2) \in \mathbb{Z}^5 \ : \\ w_i \equiv a_i z_2 \pmod{q}, \ z_1 \equiv c_0 z_2 \pmod{q}\}$$

and

$$D^* = \{(w_1, w_2, w_3, z_1, z_2) \ : \ \sum_{i=1}^{3} 6H^i|w_i| + 6H|z_1| + 6H^2|z_2| \leq 1\}.$$

2nd phase of the proof (Case 2: $\lambda_5 > 1$)

Recall that, since $\lambda_5 > 1$, we must have

$$\lambda_1^* \ll 1.$$

2nd phase of the proof (Case 2: $\lambda_5 > 1$)

Recall that, since $\lambda_5 > 1$, we must have

$$\lambda_1^* \ll 1.$$

This implies that there exist $(w_1, w_2, w_3, z_1, z_2)$ satisfying

$$w_i \ll \frac{q}{H^i}, \quad z_1 \ll \frac{q}{H} \quad z_2 \ll \frac{q}{H^2},$$

and

$$a_i z_2 \equiv w_i \pmod{q}, \quad \text{and} \quad c_0 z_2 \equiv z_1 \pmod{q}.$$

2nd phase of the proof (Case 2: $\lambda_5 > 1$)

Now, if $(x, y) \in [-H, H] \times [-H, H]$ satisfies

$$y^2 - c_0 y \equiv a_3 x^3 + a_2 x^2 + a_1 x \pmod{q},$$

we have

$$z_2 y^2 - z_1 y = w_3 x^3 + w_2 x^2 + w_1 x + qt.$$

2nd phase of the proof (Case 2: $\lambda_5 > 1$)

Now, if $(x, y) \in [-H, H] \times [-H, H]$ satisfies

$$y^2 - c_0 y \equiv a_3 x^3 + a_2 x^2 + a_1 x \pmod{q},$$

we have

$$z_2 y^2 - z_1 y = w_3 x^3 + w_2 x^2 + w_1 x + qt.$$

There can, at most, exist $O(1)$ possible choices for t and for each such value of t we apply Bombieri-Pila's result, which gives

$$|\mathcal{X}| \ll H^{1/3+o(1)}.$$

Thank you for your attention!