Sums of two cubes

Ari Shnidman
(joint work with Levent Alpöge and Manjul Bhargava)

Hebrew University of Jerusalem
ICTS–ECL 2022

August 15, 2022

Sums of two cubes

Q: Which integers can be written as a sum $x^2 + y^2$ of two integer/rational squares?

A: Those whose prime factorizations have all primes $p \equiv 3 \pmod 4$ appearing with even exponent (Girard/Fermat/Euler).

Q: Which integers can be written as a sum $x^3 + y^3$ of two cubes?

- It matters now whether we allow x and y to be rational
  - e.g. $6 = \left(\frac{17}{21}\right)^3 + \left(\frac{37}{21}\right)^3$.
- The first few are $1, 2, 6, 7, 8, 9, 12, 13, 15, 16, 17, 19, 20, 22, 26, 27, 28, \ldots$
- There seems to be no precise rule!

New question: how many **integers are a sum of two rational cubes?**

Easy to see that 0% of integers are a sum of two *integer* cubes.

Main theorem

Theorem (Alpöge-Bhargava-S)

When ordered by their absolute values, a positive proportion of integers are the sum of two rational cubes, and a positive proportion of integers are not.

More precisely, we prove that

$$\liminf_{X\to\infty} \frac{\#\{n \in \mathbb{Z} : |n| < X \text{ and } n \text{ is the sum of two rational cubes}\}}{\#\{n \in \mathbb{Z} : |n| < X\}} \geq \frac{2}{21}$$

and

$$\liminf_{X\to\infty} \frac{\#\{n \in \mathbb{Z} : |n| < X \text{ and } n \text{ is not the sum of two rational cubes}\}}{\#\{n \in \mathbb{Z} : |n| < X\}} \geq \frac{1}{6}$$

Conjecture: One half of all integers are a sum of two cubes.

Ranks in cubic twists families of elliptic curves

The equation $x^3 + y^3 = n$ is an affine model of the elliptic curve $x^3 + y^3 = nz^3$.

The elliptic curves vary through the cubic twists of the Fermat cubic $x^3 + y^3 = z^3$.

How many of these cubic twists have a (non-trivial) rational point? We prove:

Theorem (Alpöge-Bhargava-S)

Fix $d \neq 0$ and consider the cubic twist family $E_{d,n} : y^2 = x^3 + dn^2$ as $n \to \infty$. Then:

1. *At least $1/6$ of the elliptic curves $E_{d,n}$ have rank 0,*
2. *At least $1/6$ of the elliptic curves $E_{d,n}$ with good reduction at 2 have rank 1.*

Note: the curve $x^3 + y^3 = n$ is isomorphic to $y^2 = x^3 - 432n^2$ (the case $d = -432$).
Easy fact: for 100% of n, the torsion subgroup of $E_{d,n}(\mathbb{Q})$ is trivial.

Average size of the 2-Selmer group

A key ingredient is the determination of the average size of $\mathrm{Sel}_2(E_{d,n})$.

Theorem (Alpöge-Bhargava-S)

Fix $d \neq 0$ and let n range over integers satisfying any finite set (or even "acceptable" infinite sets) of congruences conditions. Then $\mathrm{avg}_n \#\mathrm{Sel}_2(E_{d,n}) = 3$.

Corollary: In any cubic twist family of elliptic curves, we have $\mathrm{avg}_n \operatorname{rk} E_{d,n}(\mathbb{Q}) \leq \frac{4}{3}$.

Corollary: The average rank is bounded in (almost) any twist family of elliptic curves:

- quadratic twist families:
  - Smith (generic case)
  - Bhargava-Klagsbrun-Lemke Oliver-S (in the presence of a 3-isogeny)
- cubic twists: Alpöge-Bhargava-S
- quartic twists: Kane-Thorne
- sextic twists: Bhargava-Elkies-S

Plan for rest of talk

1. I'll explain how to deduce our main results from $\text{avg}_n \#\text{Sel}_2(E_{d,n}) = 3$
2. I'll sketch a proof that $\text{avg}_n \#\text{Sel}_2(E_{d,n}) = 3$.

From Selmer groups to sums of two squares

Fix d and let $E_n = E_{d,n} : y^2 = x^3 + dn^2$. We have

$$0 \to E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \to \mathrm{Sel}_2(E_n) \to Ш(E_n)[2] \to 0$$

Our result that $\mathrm{avg}_n \#\mathrm{Sel}_2(E_n) = 3$ immediately implies that $\mathrm{avg}_n \, \mathrm{rk}\, E_n(\mathbb{Q}) \leq 1.5$.

(Use the inequality $r \leq \frac{1}{2} \cdot 2^r$, valid for all integers $r \geq 0$.)

But this is not enough to conclude that a positive proportion of twists have rank 0 and a positive proportion have rank 1!

For example, it could be that 50% have rank 1 and 50% have rank 2.

Root number and parity

Let $w_n \in \{\pm 1\}$ be the root number of E_n, so that

$$L(E_n, s) = w_n L(E_n, 2-s)$$

It follows from BSD that $(-1)^{\operatorname{rk} E_n} = w_n$, but the parity conjecture is open.

We use instead the p-parity theorem:

Theorem (Dokchitser-Dokchitser and Nekovář)

Let $E/\mathbb{Q}$ be an elliptic curve and let $w(E)$ be its root number. Then for every prime p,

$$w(E) = (-1)^{\dim_{\mathbb{F}_p} \operatorname{Sel}_p(E) + \dim_{\mathbb{F}_p} E[p](\mathbb{Q})}.$$

Thus, for 100% of integers n, we have

$$w_n = (-1)^{\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E_n)}$$

Root number equidistribution

We prove that the root number is equidistributed in cubic twist families and (crucially) even if we restrict to appropriate congruence sub-families:

Theorem (Alpöge-Bhargava-S)

Fix d and let $S \subset \mathbb{Z}^+$ defined by finitely many prime-to-3 congruence conditions. Then the root number w_n is equidistributed: we have $w_n = +1$ (resp. -1) for 50% of $n \in S$.

On the other hand, we show:

Theorem

Fix d and let S be an acceptable subset of $\mathbb{Z}^+$. The set $S_+ \subset S$ (resp., S_-) of $n \in S$ such that $E_{d,n}$ has root number $+1$ (resp., -1) is a countable union of acceptable sets.

We use explicit formulas of Rohrlich/Varilly-Alvarado. Up to local factors at $p \mid 6d$,

$$w_n \doteq (-1)^{\omega_{2,3}(n)}$$

where $\omega_{2,3}(n)$ is the number of primes p dividing n with $3 \nmid v_p(n)$ and $p \equiv 2 \pmod 3$.

Proof that at least $\frac{1}{6}$ of twists E_n have rank 0

- Consider the subset $S \subset \mathbb{Z}$ of n such that $w_n = 1$.
- We have $\operatorname{avg}_{n \in S} \#\mathrm{Sel}_2(E_n) = 3$.
- By 2-parity, the integer $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_n)$ is even for $n \in S$.
- Thus, at least $\frac{1}{3}$ of E_n (for $n \in S$) have $\#\mathrm{Sel}_2(E_n) = 1$ (solve $1q + 4(1-q) \leq 3$).
- Since $\frac{1}{2} \cdot \frac{1}{3} = \frac{1}{6}$, we get at least $\frac{1}{6}$ of curves with rank 0.

Proof that at least $\frac{5}{12}$ of twists E_n have 2-Selmer rank 1

- Consider the subset $S \subset \mathbb{Z}$ of n such that $w_n = -1$.
- We have $\mathrm{avg}_{n \in S} \#\mathrm{Sel}_2(E_n) = 3$.
- By 2-parity, the integer $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_n)$ is odd for $n \in S$.
- Thus, at least $\frac{5}{6}$ of E_n (for $n \in S$) have $\#\mathrm{Sel}_2(E_n) = 2$ (solve $2q + 8(1-q) \leq 3$)
- Since $\frac{1}{2} \cdot \frac{5}{6} = \frac{5}{12}$, we get at least $\frac{5}{12}$ of curves with $\#\mathrm{Sel}_2(E_n) = 2$.

Question: If $\#\mathrm{Sel}_2(E_n) = 2$, then is the rank of E_n equal to 1?

If we assume the finiteness of $Ш(E_n)$ then yes, but this is not known in general.

A p-converse theorem

However, we can use the following recent p-converse result of Burungale-Skinner.

Theorem (Burungale-Skinner)

Let $E/\mathbb{Q}$ be a CM elliptic curve with supersingular reduction at p. If $\#\mathrm{Sel}_p(E) = p$ and the map $\mathrm{Sel}_p(E) \to E(\mathbb{Q}_p)/pE(\mathbb{Q}_p)$ is injective, then $\mathrm{rk}\, E(\mathbb{Q}) = 1$.

- Notice the good reduction hypothesis.
- When $d = -432$, exactly $\frac{4}{7}$ of the curves E_n (with $n \in S$) have good reduction at 2.
- We show at least $\frac{1}{3}$ of those satisfy $\#\mathrm{Sel}_2(E) = 2$ and $\mathrm{Sel}_2(E) \hookrightarrow E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)$.
- So the total proportion of rank 1 twists we can guarantee is $\frac{1}{2}\frac{1}{3}\frac{4}{7} = \frac{2}{21}$.

Note: not all cubic twist families have curves with good reduction at 2.

Proof that $\text{avg}_n \#\text{Sel}_2(E_n) = 3$

Let E be an elliptic curve over $\mathbb{Q}$.

The Selmer group $\text{Sel}_2(E)$ parameterizes isomorphism classes of pairs (C, D) where

- $C/\mathbb{Q}$ is a genus one curve with $\text{Pic}^0(C) \simeq E$,
- D is a degree two divisor on C (up to linear equivalence), and
- $C(\mathbb{Q}_p) \neq \varnothing$ for all $p \leq \infty$.

Cohomologically:

$$\text{Sel}_2(E) = \ker\left(H^1(\mathbb{Q}, E[2]) \to \prod_p H^1(\mathbb{Q}_p, E)\right)$$

A parameterization of Bhargava-Ho

Let $G = \mathrm{SL}_2^2$ and $V = \mathrm{Sym}^3(2) \otimes (2)$, the space of pairs (f_1, f_2) of binary cubic forms.

Invariants: we have $\mathbb{C}[V]^G = \mathbb{C}[A_1, A_3]$, where A_1 and A_3 have degrees 2 and 6.

Given $(f_1, f_2) \in V(\mathbb{Q})$, we can construct a genus one hyperelliptic curve

$$C : z^2 = \mathrm{Disc}_{x,y}(f_1 x_1 + f_2 x_2)$$

We say (f_1, f_2) is *locally soluble* if $C(\mathbb{Q}_p) \neq \varnothing$ for all $p \leq \infty$.

Theorem (Bhargava-Ho)

Let $E = E(a_1, a_3) : y^2 + a_1 xy + a_3 y = x^3$. Then there is a bijection

$$\mathrm{Sel}_2(E) \longleftrightarrow G(\mathbb{Q}) \backslash V(\mathbb{Z})^{\text{loc. sol.}}_{a_1, a_3}$$

between $\mathrm{Sel}_2(E)$ and the locally soluble orbits with invariants $A_1 = a_1$ and $A_3 = a_3$.

Fact: $E(a_1, a_3)$ is the universal family of elliptic curves with a point of order 3.

2-Selmer elements for $E_{16,n}$

Let $Y \subset V$ be the G-invariant quadric defined by $A_1 = 0$.
For $y \in Y(\mathbb{Q})$, we let $\mathrm{Disc}(y) = A_3(y)$ be its *discriminant*.

Theorem (Bhargava-Ho)

Let $E^n : y^2 + ny = x^3$. Then there is a bijection

$$\mathrm{Sel}_2(E^n) \longleftrightarrow G(\mathbb{Q}) \backslash Y(\mathbb{Z})_n^{\text{loc. sol.}}$$

between $\mathrm{Sel}_2(E^n)$ and the locally soluble orbits on $Y(\mathbb{Z})$ of discriminant n.

One checks that E^n is isomorphic to the curve $E_{16,n} : y^2 = x^3 + 16n^2$ from earlier.

2-Selmer elements for $E_{d,n}$

What about for general twist families $E_{d,n}$? These don't have a 3-torsion point.

However, $E_{d,n}[2] \simeq E^{2d^2n}[2]$ and hence $H^1(\mathbb{Q}, E_{d,n}[2]) \simeq H^1(\mathbb{Q}, E^{2d^2n}[2])$.
(compare $y^2 = x^3 + dn^2$ with $y^2 = x^3 + 64d^4n^2$)

We say $(f_1, f_2) \in V(\mathbb{Q})$ is d-locally soluble if $dz^2 = \mathrm{Disc}(f_1x_1 + f_2x_2)$ is locally soluble.

Theorem (Alpöge-Bhargava-S)

Fix $d \neq 0$ and let $E_{d,n} : y^2 = x^3 + dn^2$. Then there is a bijection

$$\mathrm{Sel}_2(E_{d,n}) \longleftrightarrow G(\mathbb{Q})\backslash Y(\mathbb{Z})_{2d^2n}^{\text{d−loc. sol.}}$$

between $\mathrm{Sel}_2(E_{d,n})$ and d-locally soluble orbits on $Y(\mathbb{Z})$ of discriminant $2d^2n$.

The number of integral $G(\mathbb{Q})$-orbits in a quadric of bounded invariant

We've reduced the computation of $\mathrm{avg}_n \#\mathrm{Sel}_2(E_{d,n})$ to counting $G(\mathbb{Z})$-orbits on $Y(\mathbb{Z})$ with bounded discriminant and satisfying certain congruence conditions.

Theorem (Alpöge-Bhargava-S)

Let $S \subset \mathbb{Z}$ be defined by congruence conditions. The number of irreducible $G(\mathbb{Z})$-orbits on $Y(\mathbb{Z})$ with $A_3(y) < X$ and with $A_3(y) \in S$ is

$$N(S;X) = X \cdot \int_{\substack{y \in G(\mathbb{Z})\backslash Y(\mathbb{R}) \\ |A_3(y)|<1}} dy \cdot \prod_p \int_{y \in S_p} dy + o(X), \tag{1}$$

where dy is the measure on $Y(\mathbb{R})$ or $Y(\mathbb{Z}_p)$ given by $dr_2\, dr_3 \cdots dr_8 / (\partial A_1/\partial r_1)$, and $r_1, \ldots, r_8$ are the coordinates on V. The measure dy on $Y(\mathbb{R})$ (resp. on $Y(\mathbb{Z}_p)$) is a $G(\mathbb{R})$-invariant (resp. $G(\mathbb{Z}_p)$-invariant) measure.

Remarks on the counting-in-a-quadric result

- The main tools are Bhargava's averaging method in geometry-of-numbers and the circle method (following Heath-Brown).
- The basic idea goes back to the Alpöge's and Sam Ruth's theses, which we push a bit further (see recent talks of Alpöge and Bhargava for more details).
- Irreducible means that $\mathrm{Disc}(f_1x_1 + f_2x_2)$ has no linear factor. Such orbits always correspond to the identity element of the Selmer group.
- For the Selmer group application, we need (and prove) a more general version of this theorem allowing congruence conditions and weighted counts.
- With these weights and congruence conditions, a "standard" argument shows that the Euler product is 2. Since $1 + 2 = 3$, we find that $\mathrm{avg}_n \#\mathrm{Sel}_2(E_{d,n}) = 3$.
- This finishes a sketch of the proof of the "sum of two cubes" result.

Proof of Selmer parameterization

In the remaining time, let's sketch a proof of:

Theorem (Alpöge-Bhargava-S)

Fix $d \neq 0$ and let $E_{d,n} : y^2 = x^3 + dn^2$. Then there is a bijection

$$\mathrm{Sel}_2(E_{d,n}) \longleftrightarrow G(\mathbb{Q})\backslash Y(\mathbb{Z})^{\text{d-loc. sol.}}_{2d^2n}$$

between $\mathrm{Sel}_2(E_{d,n})$ and d-locally soluble orbits on $Y(\mathbb{Z})$ of discriminant $2d^2n$.

The main question is: why do all elements of $\mathrm{Sel}_2(E_{d,n})$ have the form $dz^2 = \mathrm{Disc}(f_1x_1 + f_2x_2)$, for some $(f_1, f_2) \in Y(\mathbb{Z})$?

Let $\tilde{G} = \mathrm{GL}_2^2$. Under the bijection of Bhargava-Ho:

$$\mathrm{Sel}_2(E^n) \longleftrightarrow G(\mathbb{Q})\backslash Y(\mathbb{Z})_n^{\text{loc. sol.}}$$

we have $\mathrm{Stab}_{\tilde{G}}(f_1, f_2) \simeq \Theta(\mathscr{L}_n)$, where $\mathscr{L}_n$ is the line bundle $\mathcal{O}_{E^n}(2\infty)$ and $\Theta(\mathscr{L}_n)$ is the automorphism group of $\mathscr{L}_n$ over E^n. We have:

$$0 \to \mathbb{G}_m \to \Theta(\mathscr{L}_n) \to E^n[2] \to 0$$

Lemma ("Arithmetic Invariant Theory")

The $G(\mathbb{Q})$-orbits on $Y(\mathbb{Q})$ of discriminant n are in bijection with $H^1(\mathbb{Q}, \Theta(\mathscr{L}_n))$.

We also have

$$\mathrm{Sel}_2(E^n) \subset H^1(\mathbb{Q}, \Theta(\mathscr{L}_n)) \subset H^1(\mathbb{Q}, E^n[2])$$

Isomorphism of Theta groups

Now let $A = E_{d,1}$. We saw $\eta\colon A[2] \simeq E^m[2]$, where $m = 2d^2$.

Theorem

Let $\mathscr{L}_A = \mathcal{O}_A(2\infty)$. Then $\Theta(\mathscr{L}_A) \simeq \Theta(\mathscr{L}_m)$ as central extensions.

Proof idea.

Consider $\mathscr{M} = \mathscr{L}_A \boxtimes \mathscr{L}_m$ on $A \times E^m$, which is the pullback of a principal polarization from $B = (A \times E^m)/\Gamma_\eta$. Now consider $\Theta(\mathscr{M})$ and use the theory of Theta groups and descent of line bundles [Mumford, §23]. □

It follows that $H^1(\mathbb{Q}, \Theta(\mathscr{L}_A)) \simeq H^1(\mathbb{Q}, \Theta(\mathscr{L}_m))$, and moreover this is compatible with the inclusion of Selmer groups. We can therefore realize every element of $\mathrm{Sel}_2(A)$ as coming from a $G(\mathbb{Q})$-orbit of V. We then need to show integrality...

Generalization to higher dimensional cubic twist families

Theorem

Let A be an abelian variety over $\mathbb{Q}$ with a degree 4 polarization $\lambda\colon A \to \widehat{A}$ induced by a symmetric line bundle $\mathscr{L} \in \mathrm{Pic}(A)$. Suppose $(A, \mathscr{L})$ admits a μ_3-action, and for each non-zero $n \in \mathbb{Z}$, let $\lambda_n : A_n \to \widehat{A}_n$ be the cubic twist of λ. Then $\mathrm{avg}_n \#\mathrm{Sel}_{\lambda_n}(A_n) = 3$.

Example: Let $C : y^3 = x^4 + ax^2 + b$, a genus three curve.

- C admits a double cover to the elliptic curve $E : y^3 + x^2 + ax + b$.
- Let $A = \ker(\mathrm{Jac}(C) \to E)$ be the corresponding Prym variety.
- Then A is an abelian surface satisfying all the conditions above.

Ranks of cubic twists of abelian surfaces

Corollary

Fix $a, b \in \mathbb{Q}$ and let A_n be the Prym variety of $ny^3 = x^4 + ax^2 + b$. Then the average rank of $A_n(\mathbb{Q})$ is at most 3.

Proof.

- The polarization $\lambda \colon A \to \widehat{A}$ is not multiplication by 2.
- But $\widehat{A}$ is the Prym of the dual curve $y^3 = x^4 + 8ax^2 + 16(a^2 - 4b)$.
- The polarization $\tilde{\lambda} \colon \widehat{A} \to A$ composes to multiplication by 2 on A.
- Our result gives $\operatorname{avg}_n \operatorname{Sel}_{\lambda_n}(A_n) = 3$ and $\operatorname{avg}_n \operatorname{Sel}_{\tilde{\lambda}_n}(\widehat{A}) = 3$.
- It follows that the average rank of $\operatorname{Sel}_2(A_n)$ is at most 3.

□

The abelian surfaces A all have quaternionic multiplication by the quaternion order of discriminant 6. What can one say about the root numbers of such abelian surfaces?

Thank you!

Proof details

There is a short exact sequence

$$1 \to \mathbb{G}_m \longrightarrow \Theta(\mathscr{M}) \xrightarrow{p} A[\lambda] \times E[2] \longrightarrow 1.$$

Let $\pi: A \times E \to B$ be the quotient map. The subgroup $\Gamma_\eta \subset A[\lambda] \times E[2]$ is maximal isotropic with respect to the skew-symmetric Weil pairing induced by $\mathscr{M}$, since

$$\langle (P, \eta(P)), (Q, \eta(Q)) \rangle_{\mathscr{M}} = \langle P, Q \rangle_{\mathscr{L}_A} \langle \eta(P), \eta(Q) \rangle_{\mathscr{L}_E} = \langle P, Q \rangle^2_{\mathscr{L}_A} = 1.$$

Let $\pi: A \times E \to B$ be the quotient map. There is therefore a line bundle $\mathscr{L}_B$ on B such that $\pi^* \mathscr{L}_B \simeq \mathscr{M}$. The existence of $\mathscr{L}_B$ implies that there is a subgroup $H \subset \Theta(\mathscr{M})$ and an isomorphism $\psi: \Gamma_\eta \simeq H$ such that $p \circ \psi = \mathrm{id}$.
This data determines an isomorphism $\tilde{\eta}: \Theta(\mathscr{L}_A) \to \Theta(\mathscr{L}_n)$ of theta groups. Explicitly, if $\psi(P, \eta(P)) = (P, s_0, \eta(P), r_0) \in H \subset \Theta(\mathscr{M})$, then

$$\tilde{\eta}(P, s) = (\eta(P), (s_0^{-1} s) r_0)$$

where we view $s_0^{-1} s$ as a scalar in $\mathrm{Aut}(\mathscr{L}_A) \simeq \mathbb{G}_m \simeq \mathrm{Aut}(\mathscr{L}_E)$.