Integers that are the sum of two rational cubes

Manjul Bhargava
Princeton University

(Joint work with Levent Alpöge and Ari Shnidman)

VaNTAGe Seminar

May 31, 2022

Which integers are the sum of two rational cubes?

It is well-known which integers are the sum of two rational squares. Such integers have density zero. Moreover, an integer is the sum of two rational squares if and only if it is the sum of two integer squares, and this occurs precisely when there is no local obstruction.

In contrast, the integers that are the sum of two rational cubes do not seem to follow any simple pattern:

$1, 2, 6, 7, 8, 9, 12, 13, 15, 16, 17, 19, 20, 22, 26, 27, 28, 30, 31, 33, 34, 35, \ldots$

In particular, it has not been known whether this set has strictly positive density, or density strictly less than 1!

In contrast to the situation for squares, it is possible for an integer to be the sum of two rational cubes but not the sum of two integer cubes: the smallest example is $6 = (17/21)^3 + (37/21)^3$.

There is never any local obstruction for an integer to be the sum of two rational cubes. Therefore, proving results on the density of this set must require global arguments.

What is the expected density?

Note that the equation $E_n : x^3 + y^3 = nz^3$ defines an elliptic curve over $\mathbb{Q}$.

If $|n| > 2$, then E_n has no nontrivial rational torsion.

Therefore, for such integers n, we have that n is the sum of two rational cubes if and only if E_n has positive rank.

What are the expected ranks of E_n? By the Minimalist Conjecture (Goldfeld, Katz–Sarnak, Bektemirov–Mazur–Stein–Watkins), in a "random" family of elliptic curves, we expect half of the curves in the family to have rank 0, half to have rank 1, and 0% to have rank ≥ 2.

The reason behind this conjecture is: we don't expect an elliptic curve to have rat'l points unless it is forced to by its root number. If the curves are random, we expect half of all curves to have root number $+1$ and half -1 $\implies$ 50% should have rank 0, 50% rank 1.

Thus, it is natural to expect that a density of $1/2$ of all integers should be the sum of two rational cubes.

Main results

Theorem (Alpöge, B., Shnidman)

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

More precisely, we prove that

$$\liminf_{X\to\infty} \frac{\#\{n\in\mathbb{Z} : |n| < X \text{ and } n \text{ is the sum of two rational cubes}\}}{\#\{n\in\mathbb{Z}\colon |n| < X\}} \geq \frac{1}{12}.$$

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

Main results (cont'd)

The theorem is equivalent to the statement that, in the family of cubic twists $x^3 + y^3 = nz^3$ of the Fermat elliptic curve, at least $1/6$ have rank zero, and at least $1/12$ have rank one.

More generally, we may consider general families of cubic twists of elliptic curves. Such a cubic twist family is of the form $E_{d,n}\colon y^2 = x^3 + dn^2$, where $d \in \mathbb{Z}$ is fixed and $n \in \mathbb{Z}$ varies.

Since the elliptic curve $x^3 + y^3 = n$ can be expressed in Weierstrass form as $y^2 = x^3 - 432n^2$, this family corresponds to the case $d = -432$.

Theorem (Alpöge, B., Shnidman)

Fix $d \neq 0$. Then, when n varies ordered by $|n|$, at least $1/6$ of the elliptic curves in the cubic twist family $E_{d,n} : y^2 = x^3 + dn^2$ have rank 0, and at least $1/6$ of the curves with good reduction at 2 have rank 1.

Main results (cont'd)

The cubic twists families $E_{d,n} : y^2 = x^3 + dn^2$ have traditionally been studied via the Selmer groups associated to a natural isogeny $\sqrt{-3} : E_{d,n} \to E_{-27d,n}$ defined over $\mathbb{Q}$.

This allows one to determine the 3-Selmer group of any such curve. In 1879, Sylvester used this $\sqrt{-3}$-descent (see also Selmer 1951) to show that the 3-Selmer rank of $x^3 + y^3 = p$ for p a prime is 0 if $p \equiv 2, 5 \pmod 9$ and is 1 if $p \equiv 4, 7, 8 \pmod 9$.

This proved that primes $p \equiv 2, 5 \pmod 9$ are not the sum of two cubes, and led Sylvester to conjecture that primes $p \equiv 4, 7, 8 \pmod 9$ are the sum of two cubes, a proof of which was recently announced by Kriz.

The $\sqrt{-3}$-Selmer group is not very useful in studying $x^3 + y^3 = n$ when n has many factors, however, as the size of the $\sqrt{-3}$-Selmer group tends to grow with the number of prime factors:

Theorem (Alpöge, B., Shnidman)

We have $\mathrm{avg}_n \#\mathrm{Sel}_3(x^3 + y^3 = n) = \infty$.

Determining instead the average size of the 2-Selmer group

We approach the problem instead via a parametrization of and a determination of the average size of the 2-Selmer group of elliptic curves in any cubic twist family.

We then use this theorem to deduce a positive proportion of 2-Selmer rank 0 curves (and thus a positive proportion of integers that are not the sum of two rational cubes), and a positive proportion of 2-Selmer rank 1 curves which can be shown to in fact have rank 1 (implying that a positive proportion of of integers are the sum of two rational cubes).

Two key ingredients in this deduction are the p-parity theorem of Nekovar and Dokchitser–Dokchitser, and a p-converse theorem of Burungale–Skinner.

Proof that a positive proportion of integers are (resp. are not) the sum of two rational cubes

1. Parametrization of 2-Selmer elements of elliptic curves in a cubic twist family by certain integer points on an $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$-invariant quadric hypersurface in the space of triply-symmetric $2 \times 2 \times 2 \times 2$ matrices.

2. Combining geometry-of-numbers with the circle/Delta method of Ramanujan–Hardy–Littlewood–Kloosterman–Heath-Brown to count integer points on this quadric in a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$.

3. Determination of the average size of the 2-Selmer group of $E_{d,n}$ with d fixed and n varying.

4. Analysis of root numbers in the family $E_{d,n}$; proof that these root numbers are equidistributed.

5. Application of the p-Parity and the p-Converse Theorems to show that many of the curves must have rank 0 and rank 1.

2 x 2 x 2 x 2 matrices and elliptic curves (joint work with Wei Ho)

Let K be a field with $\mathrm{char}(K) \neq 2$.

Let $A \in K^2 \otimes K^2 \otimes K^2 \otimes K^2$ be a $2 \times 2 \times 2 \times 2$ matrix with entries in K.

We may then view A as a quadrilinear form on $W_1 \times W_2 \times W_3 \times W_4$, where the W_i's are two-dimensional vector spaces over K.

Consider the set

$$C_{12}(K) := \{(w_1, w_2) \in \mathbb{P}(W_1) \times \mathbb{P}(W_2) : \det(H(w_1, w_2, \cdot, \cdot)) = 0\} \subset \mathbb{P}^1 \times \mathbb{P}^1.$$

Then $C_{12}(K)$ consists of the set of K-points of a bidegree $(2, 2)$ curve C_{12} in $\mathbb{P}^1 \times \mathbb{P}^1$, which is generically a smooth genus one curve (this happens when $\mathrm{Disc}(A) \neq 0$).

In this way, we obtain six genus one curves C_{ij} in $\mathbb{P}^1 \times \mathbb{P}^1$.

2 x 2 x 2 x 2 matrices and elliptic curves (joint work with Wei Ho)

$$C_{12}(K) := \{(w_1,w_2)\in\mathbb{P}(W_1)\times\mathbb{P}(W_2) : \det(H(w_1,w_2,\cdot,\cdot))=0\}\subset\mathbb{P}^1\times\mathbb{P}^1.$$

In fact, the curve C_{12} maps into $\mathbb{P}(W_1)\times\mathbb{P}(W_2)\times\mathbb{P}(W_3)\cong\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^1$.

Given $(w_1,w_2)\in C_{12}$, since $H(w_1,w_2,\cdot\,,\cdot\,)$ is singular as a bilinear form on $W_3\times W_4$, the kernel of $H(w_1,w_2,\cdot\,,\cdot\,)$ in W_3 is non-trivial and generically one-dimensional.

We thus obtain a well-defined element $w_3\in\mathbb{P}(W_3)$ such that $H(w_1,w_2,w_3,\cdot\,)\equiv 0$. Therefore,

$$C_{123}(K) := \{(w_1,w_2,w_3)\in\mathbb{P}(W_1)\times\mathbb{P}(W_2)\times\mathbb{P}(W_3) : H(w_1,w_2,w_3,\cdot)\equiv 0\}$$

gives the set of K-points of a genus one curve C_{123} in $\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^1$.

The projection of C_{123} onto $\mathbb{P}(W_1)\times\mathbb{P}(W_2)$ gives an isomorphism onto C_{12}. Thus C_{123} provides us with explicit isomorphisms among the three curves C_{12}, C_{13}, and C_{23}, via projection and unprojection.

2 x 2 x 2 x 2 matrices and elliptic curves (joint work with Wei Ho)

$$C_{123}(K) := \{(w_1, w_2, w_3) \in \mathbb{P}(W_1)\times\mathbb{P}(W_2)\times\mathbb{P}(W_3) : H(w_1, w_2, w_3, \cdot) \equiv 0\}$$

We similarly have curves C_{124}, C_{134}, and C_{234} in $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$.

We thus obtain a tetrahedron of maps:

$$\begin{tikzcd}
 & C_{123} \arrow[dl, leftrightarrow] \arrow[dr, leftrightarrow] \arrow[dd, leftrightarrow] & \\
C_{124} \arrow[rr, leftrightarrow, dashed] \arrow[dr, leftrightarrow] & & C_{134} \arrow[dl, leftrightarrow] \\
 & C_{234} &
\end{tikzcd}$$

However, these isomorphisms do not all commute with each other!

2 x 2 x 2 x 2 matrices and elliptic curves (joint work with Wei Ho)

$$\begin{tikzcd}
 & C_{123} \arrow[dl, <->] \arrow[dr, <->] \arrow[dd, <->] & \\
C_{124} \arrow[rr, <->, dashed] \arrow[dr, <->] & & C_{134} \arrow[dl, <->] \\
 & C_{234} &
\end{tikzcd}$$

For example, starting at C_{123} and tracing around triangle j yields a hyperelliptic involution ι_j ($j = 1, 2, 3$) on C_{123}.

If one instead starts at C_{123} and follows a quadrilateral of isomorphisms involving all four curves, then (viewing the traversal of the quadrilateral as a traversal of two triangles) we obtain the automorphism $\iota_i \circ \iota_j$ of C_{123}, which is a translation of C_{123} by a point P_{ij} on the Jacobian of C_{123}.

2 x 2 x 2 x 2 matrices and elliptic curves (joint work with Wei Ho)

We thus obtain three points P_{12}, P_{23}, and P_{31} on the Jacobian $E := E(A)$ of $C := C_{123}$. Since $(\iota_1 \circ \iota_2) \circ (\iota_2 \circ \iota_3) \circ (\iota_3 \circ \iota_1) = \mathrm{id}$,

$$P_{12} + P_{23} + P_{31} = 0.$$

Let D_i be a degree two divisor on C_{123} corresponding to the projection onto $\mathbb{P}(W_i)$.

Then $\iota_i \circ \iota_j(x) = x + (D_i - D_j)$, so that $P_{ij} = D_i - D_j$.

Theorem (B., Ho)

There is a canonical bijection between nondegenerate $\mathrm{GL}_2(K)^4$-orbits on the space $K^2 \otimes K^2 \otimes K^2 \otimes K^2$ and isomorphism classes of triples $(C, L, (P, P', P''))$, where C is a smooth irreducible genus one curve over K, L is a degree 2 line bundle on C, and P, P', P'' are nonzero K-points that sum to zero in $\mathrm{Pic}^0(C)(K)$.

Triply-symmetric 2 x 2 x 2 x 2 matrices and elliptic curves with a marked point of order 3

Theorem (B., Ho)

There is a canonical bijection between nondegenerate $\mathrm{GL}_2(K)^2$-orbits on the space $K^2 \otimes \mathrm{Sym}_3 K^2$ of pairs of binary cubic forms and isomorphism classes of triples (C, L, P), where C is a smooth genus one curve over K, L is a degree 2 line bundle on C, and P is a nonzero 3-torsion point on the Jacobian of C defined over K.

There are two polynomial invariants for the action of SL_2^2 on pairs of binary cubic forms, of degrees 2 and 6, which we call a_1 and a_3, respectively.

The Jacobian of the curve C corresponding to A under the above bijection has equation

$$E = \mathrm{Jac}(C) : y^2 + a_1 xy + a_3 y = x^3.$$

Triply-symmetric 2 x 2 x 2 x 2 matrices and elliptic curves with a marked point of order 3

A $2 \times 2 \times 2 \times 2$ integer matrix is locally soluble if the corresponding genus one curve C has points everywhere locally.

Theorem (B., Ho)

The elements in the 2*-Selmer group* $S_2(E)$ *of*

$$E : y^2 + a_1xy + a_3y = x^3$$

are in bijection with $\mathrm{SL}_2^2(\mathbb{Q})$*-equivalence classes on the set of locally soluble elements of the space* $\mathbb{Z}^2 \otimes \mathrm{Sym}_3\mathbb{Z}^2$ *of pairs of integral binary cubic forms having invariants equal to the coefficients* $M^i a_i$ *of* E *for some fixed integer* M*.*

Corollary

The elements in the 2*-Selmer group* $S_2(E)$ *of* $E : y^2 = x^3 + 16n^2$ *are in bijection with* $\mathrm{SL}_2^2(\mathbb{Q})$*-equivalence classes on the set of locally soluble pairs of integral binary cubic forms having vanishing* a_1*-invariant and* $a_3 = M^3n$ *for a fixed integer* M*.*

A quadric hypersurface in the space of 2 x 2 x 2 x 2 matrices and a cubic twist family of elliptic curves

Theorem (Alpöge, B., Shnidman)

The elements in the 2-Selmer group $S_2(E)$ of $E_{d,n} : y^2 = x^3 + dn^2$ are in bijection with $\mathrm{SL}_2^2(\mathbb{Q})$-equivalence classes on the set of integral pairs of binary cubic forms satisfying certain congruence conditions, having vanishing a_1-invariant, and $a_3 = M^3 n$ for a fixed integer $M = M_d$.

We thus must count a certain weighted number of integer points, satisfying certain congruence conditions, lying on the quadric $a_1 = 0$, in a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})^2$ on the 8-dimensional space of real pairs of binary cubic forms.

We use geometry-of-numbers techniques to count these integer points in this unbounded but finite-volume region, invoking the circle/Delta method of Kloosterman–Heath-Brown. This combination of techniques was first studied by Sam Ruth in his thesis on the space of binary quartic forms, and written in a very generally applicable form by Levent Alpöge in his thesis.

The average size of the 2-Selmer group in a family of cubic twists

We thus use geometry of numbers together with the circle method as in Alpöge's thesis: in the "main body" of the fundamental domain the circle/Delta method is applicable and we use it to count integral zeroes of our quadratic form in an approximate cube in $\mathbb{R}^8$.

Then in the majority of the cusp of the fundamental domain, we apply a divisor bound to bound the point count by something which is suboptimal but sufficiently sharp to conclude (because the volume integral for the fundamental domain converges quickly).

Finally, deep in the cusp, we show that that the integral points on the quadric correspond to identity elements of the Selmer group, which can be counted separately.

A quadric hypersurface in the space of 2 x 2 x 2 x 2 matrices and a cubic twist family of elliptic curves (cont'd)

The local densities are computed and found to agree with those arising in previous work on the average size of the 2-Selmer group across the universal family elliptic curves (as studied in previous works of B.-Shankar and B.-Ho). Thus, we prove, in this thin set too:

Theorem

Fix $d \neq 0$. When $n \in \mathbb{Z}$ varies ordered by $|n|$, the average size of $\mathrm{Sel}_2(E_{d,n} : y^2 = x^3 + dn^2)$ is 3.

The same average holds when ranging over n satisfying any finite set (or even suitable infinite sets) of congruence conditions.

Root number analysis in families of cubic twists

Theorem

Ordering by $|n|$, half the curves $x^3 + y^3 = n$ have root number $+1$, and half have root number -1.

We show that curves having only root number $+1$ (resp. -1) can be extracted from the family $E_{d,n}$ by congruence conditions on n.

Ignoring 2 and 3, the root number of $y^2 = x^3 - 432n^2$ is (Rohrlich, Várilly-Alvarado) $\sim (-1)^{\omega_{2 \bmod 3}(n)}$ where $\omega_{2 \bmod 3}(n)$ is the number of $2 \bmod 3$ primes dividing n (without multiplicity).

If n is squarefree and prime to 3, then $(-1)^{\omega_{2 \bmod 3}(n)} \equiv n \pmod 3$, so it's easy to get a positive proportion with given root number! Explicitly, we can use this to show, e.g., that the root number is $+1$ if n is squarefree and $1 \pmod 9$.

The theorem follows from obtaining cancellation in $\sum_n (-1)^{\omega_{2 \bmod 3}(n)}$, which we carry out via the Selberg–Delange method.

Average size of the 2-Selmer group for curves with given root number

Because we can extract all root number $+1$ curves in the family $E_{d,n}$ by (unions of) sets defined by congruence conditions on n:

Theorem

Fix $d \geq 0$. The average size of the 2-Selmer group of $E_{d,n} : y^2 = x^3 + dn^2$, as n varies, is 3, even if one restricts to just those n where the root number of $E_{d,n}$ is $+1$ (resp. -1).

We may now apply the p-Parity Theorem (Nekovar and Dokchitser–Dokchitser), which states that the 2-Selmer rank must be consistent with the root number.

Across the root number $+1$ curves, the 2-Selmer group size will always be an even power of 2 (i.e., 1, 4, 16, etc.), while for the root number -1 curves, the 2-Selmer group size will always be an odd power of 2 (i.e., 2, 8, 32, etc.).

Applying the p-Parity Theorem

Since the average size of $\mathrm{Sel}_2(E_{d,n})$ is 3 across those $E_{d,n}$ having root number $+1$, by the p-Parity Theorem of Nekovar and Dokchitser–Dokchitser, we conclude that at least $1/3$ of these curves must have 2-Selmer rank 0 (note that 3 is the average of $1, 4, 4$).

Corollary

Fix $d \neq 0$. As n varies ordered by absolute value, at least $1/6$ of the elliptic curves $E_{d,n}$ have 2-Selmer rank 0 and thus rank 0.

Applying the p-Parity and the p-Converse Theorems

Since the average size of $\mathrm{Sel}_2(E_{d,n})$ is 3 across those $E_{d,n}$ having root number -1, by the p-Parity Theorem of Nekovar and Dokchitser–Dokchitser, we conclude that at least $5/6$ of these curves must have 2-Selmer rank 1 (note that 3 is the average of $2, 2, 2, 2, 2, 8$).

Corollary

Fix $d \neq 0$. As n varies ordered by absolute value, at least $5/12$ of the elliptic curves $E_{d,n}$ have 2-Selmer rank 1.

Under certain technical assumptions, the p-Converse Theorem of Burungale and Skinner allows us to conclude that a curve has rank 1if it has p-Selmer rank 1.

Corollary

Fix $d \neq 0$. As n varies ordered by absolute value, at least $1/6$ of the elliptic curves $E_{d,n}$ with good reduction at 2 have rank 1.

Consequences

Corollary

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

Corollary

When ordered by absolute value, a positive proportion of integers are the product of three rational numbers in arithmetic progression, and a positive proportion are not.

etc.

Thank you!!