Non-Trivial Arithmetic Progressions of Four Squares and Three Cubes Over Q√D

Principal Investigator: Dr. Edray Herber Goins, Graduate Assistant: James Weigandt
Sergio García Currás , Ronald Archer,, Han Liu, Benito Martínez, Stephen Mussmann, Lirong Yuan
Department of Mathematical Sciences, Purdue University, West Lafayette, IN 47907

Conceptual Frame

Rational point: point on a curve whose x- and y- coordinates are both rational numbers.
Elliptic curve: Curve with an equation of the form $y^2 = x^3 + ax + b$, a, b are real numbers that has at least one rational point.
(L. J. Mordell): "The set of rational points on an elliptic curve forms a finitely generated abelian group under the tangent-secant operation."
Arithmetic progression: sequence of terms such that $a_{n+1} - a_n = d$ for any a{n}, a{n+1}, d a constant
Quadratic extension $\mathbb{Q}(\sqrt{D})$: the rational numbers plus the square root of the square-free integer D.

Preliminary results

---There are no non-constant arithmetic progressions of four squares and no non-trivial arithmetic progressions of three cubes over the rational numbers.

---Let D=mp be a square-free integer with $m \in \pm1, \pm2, \pm3, \pm6$ and p being a prime equal to or greater than five. There may be non-constant arithmetic progressions of four squares and non-trivial arithmetic progressions of three cubes over the quadratic extension $\mathbb{Q}(\sqrt{D})$.

---Let X○(24) denote the elliptic curve

$y^2 = x^3 + 5x^2 + 4x$

and let X○(36) denote the elliptic curve

$y^2 = x^3 - 27$

*There exists a bijection between arithmetic progressions of four squares over $\mathbb{Q}(\sqrt{D})$ and rational points on $X_0(24)(\mathbb{Q}\sqrt{D})$

*There exists a bijection between arithmetic progressions of three cubes over $\mathbb{Q}(\sqrt{D})$ and rational points on $X_0(36)(\mathbb{Q}\sqrt{D})$

*Thus, looking for arithmetic progressions of four squares or three cubes over $\mathbb{Q}(\sqrt{D})$ is equivalent to looking for rational points on $X_0(24)(\mathbb{Q}\sqrt{D})$ and on $X_0(36)(\mathbb{Q}\sqrt{D})$, respectively.

---Let E be an elliptic curve.

*$E(\mathbb{Q}\sqrt{D}) \cong E^D(\mathbb{Q})$

i.e., $E(\mathbb{Q}(\sqrt{D}))$ has the same structure as $E^D(\mathbb{Q})$ (they are isomorphic.)

Equivalent Problem

Because of this isomorphism, looking for rational points on $E(\mathbb{Q}(\sqrt{D}))$ is equivalent to looking for rational points on $E^D(\mathbb{Q})$.

There exists a non-constant arithmetic progression of four squares and a non-trivial arithmetic progression of three cubes over $\mathbb{Q}(\sqrt{D})$ if and only if the rank of

$X_0(24)^D(\mathbb{Q}) : y^2 = x^3 + 5Dx^2 + 4D^2x$

and the rank of

$X_0(36)^D(\mathbb{Q}) : y^2 = x^3 - 27D^3$ (1)

respectively, are positive.

Let p be a prime mod n, n an integer. Conjecturally, the ranks of an elliptic curve twisted by different values of D with the same congruence with p modulo n have the same parity. If, for example, the ranks of an elliptic curve twisted by values of D all belonging to a certain congruence class are even, these ranks can either be 0 or 2. We would like to see if for some of these classes we can prove that the rank is always 0, so that, by (1), there are no non-constant arithmetic progressions of four squares or no non-trivial arithmetic progressions of three cubes over $\mathbb{Q}(\sqrt{D})$ for any values of D in those classes.

Procedure

Let p be a prime. We checked if we could sharpen the bounds on the ranks of $X_0(24)(\mathbb{Q})$ twisted by values of D congruent to p mod 24. The method employed for this was the following:

Method

Consider the homomorphism

$$\delta: \frac{X_0^D(24)\mathbb{Q}^*}{2X_0^D(24)(\mathbb{Q}^*)^2} \rightarrow \frac{\mathbb{Q}^*}{(\mathbb{Q}^{*2})} \times \frac{\mathbb{Q}^*}{(\mathbb{Q}^{*2})}$$

$$(x : y : 1) \mapsto (x, x + D)$$

A pair (d1,d2) is in Im(δ) if and only if the system of equations

$$\begin{aligned} d_1u^2 - d_2v^2 &= -D \\ d_1u^2 - d_1d_2w^2 &= -4D \end{aligned} \qquad (2)$$

has a rational solution (u,v,w).

Because Im(δ) is a subgroup, if this system has no solution for one of the pairs (d1,d2) in a coset, then it has no solution for any pair in that coset. This way, we can narrow down the number of elements in Im(δ), obtaining lower upper bounds on the rank (since the number of elements in Im(δ) is 2^{2+r}, where r is the rank.)

We eliminate pairs from Im(δ) by checking that:
1) (2) has no real solutions.
2) One of the equations in (2) has no solutions modulo 8 or modulo 9.
3) Both equations in (2) have no solution modulo 8.

Results

p/m	1	2	3	6	-1	-2	-3	-6
1	2	2	2	3	2	2	2	2
5	0	1	0	1	1	1	1	0
7	0	0	1	1	1→0	2	1	0
11	1	1	1→0	1	0	1	1	2
13	1	0	2	1	2→0	0	2→1	0
17	1	1	1→0	1	1	1	0	0
19	0	2	0	1	1	0	1	2
23	1	1	1	1	1	1	1	2

This table shows the ranks of $X_0^D(24)(\mathbb{Q})$ with D being congruent with p mod 24.
By (1), there are no non-constant arithmetic progressions of four squares over $\mathbb{Q}(\sqrt{D})$ for values of D with a 0 in the table above.
a →b means that the upper bound of the rank of $X_0^D(24)(\mathbb{Q})$ for that particular value of D was lowered from a to b.
We lowered the upper bound in 5 cases and raised the lower bounds in 30 cases.

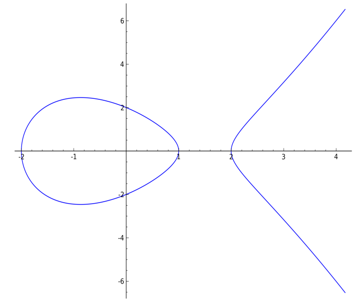
Current Research Situation

We are currently working on the proof of certain theorems which, if true, would lower the upper bounds on the ranks of $X_0^D(36)(\mathbb{Q})$ for all congruence classes p mod 36 of D. Our focus is now on raising the lower bounds on the ranks of $X_0^D(36)(\mathbb{Q})$ for these congruence classes. If the truth of these theorems can be proved, the table of the ranks of $X_0^D(36)(\mathbb{Q})$ for values of D congruent with p mod 36 would be the following:

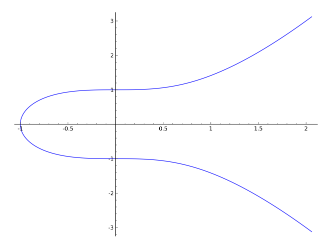
Partial results of looking at the ranks of X0^(D)(36)(Q), D congruent with p modulo 36

p/m	1	2	3	6	-1	-2	-3	-6
1	2	3	2	2	2	2	2	3
5	0	1	0	0	0	0	0	1
7	1	1	1	0	1	0	1	1
11	1	1	1	2	1	2	1	1
13	2	1	2	2	2	2	2	1
17	0	1	0	0	0	0	0	1
19	1	1	1	2	1	2	1	1
23	1	1	1	2	1	2	1	1

We only look at $X_0(36)(\mathbb{Q})$ twisted by values of D congruent with p modulo 24 because all the information that may be gathered from looking at the table of the ranks of $X_0(36)(\mathbb{Q})$ when twisted by D belonging to the congruence classes p mod 36 can be gathered from considering D in the congruence classes p mod 24.



Graph of the elliptic curve $y^2 = x^3 + 5x^2 + 4x$



Graph of the elliptic curve $y^2 = x^3 - 27$

Acknowledgements

Dr. Edray Herber Goins

The National Science Foundation