Non-Trivial Arithmetic Progressions of Four Squares and Three Cubes Over \( \mathbb{Q} \sqrt{D} \)

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

Rational point on a curve whose \( x \)- and \( y \)-coordinates are both rational numbers.
Elliptic curve: Curve with an equation of the form
\[ y^2 = x^3 + ax + b \]
where \( a, b \) are real numbers with \( \Delta = 4a^3 + 27b^2 \neq 0 \) 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 \( a(n), d(n) \) of a constant
Quadratic extension \( \mathbb{Q}(\sqrt{D}) \): the rational numbers plus the square root of the square-free integer \( D \).

---There are no non-constant arithmetic progressions of four squares and no non-trivial arithmetic progressions of three cubes over the rational numbers.
---Let \( D \) be a square-free integer with \( m \in \pm 1, \pm 2, \pm 3, \pm 6 \) 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 \( \mathbb{Q}(\sqrt{D}) \).

Procedure

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

Consider the homomorphism
\[ X_0^P(24)(\mathbb{Q}) \rightarrow \mathbb{Q}^* \times \mathbb{Q}^* \]
\[ (x : y : 1) \rightarrow (x, x + D) \]
A pair \( (d_1, d_2) \) is in \( \text{Im}(5) \) if and only if the system of equations
\[ d_1 x^2 - d_2 x = -D \]
\[ d_1 y^2 - d_2 x^2 = -4D \]
has a rational solution \( (x, y) \).
Because \( \text{Im}(5) \) is a subgroup, this system has no solution for one of the pairs \( (d_1, d_2) \) 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 \( \text{Im}(5) \), obtaining lower upper bounds on the rank. (Since the number of elements in \( \text{Im}(5) \) is \( 2^{2+r} \), where \( r \) is the rank.)

---There exists a bijection between arithmetic progressions of four squares and rational progressions of four squares over \( \mathbb{Q} \sqrt{D} \) if and only if the rank of \( X_0(D)(\mathbb{Q}) \):
\[ y^2 = x^3 + 5Dx^2 + 4D^2x \]

**Results**

| \( D \) | 1 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| \( X_0(36)(\mathbb{Q}) \) & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 |
| \( X_0(36)(\mathbb{Q}) \) & 0 & 1 | 0 & 1 | 0 & 1 | 0 & 1 | 0 & 1 | 0 & 1 |

This table shows the ranks of \( X_0^P(24)(\mathbb{Q}) \) with \( D \) being congruent with \( p \) modulo 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.

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 \( X_0^P(36)(\mathbb{Q}) \) for all congruence classes \( p \) mod 36 of \( D \). Our focus is now on raising the lower bounds on the ranks of \( X_0^P(36)(\mathbb{Q}) \) for these congruence classes. If the truth of these theorems can be proved, the table of the ranks of \( X_0^P(36)(\mathbb{Q}) \) for values of \( D \) congruent with \( p \) mod 36 would be the following:

**Acknowledgements**

Dr. Edray Herber Goins
The National Science Foundation