Good ABC Triples and Good Elliptic Curves

Elise Alvarez-Salazar[1] Calvin Henaku[2]

[1]University of California Santa Barbara [2]Washington University in St. Louis

Abstract

The Modified Szpiro Conjecture, which is an open statement about elliptic curves, is equivalent to the ABC conjecture. This equivalence gives us a dictionary that moves between good abc triples and good elliptic curves. This summer, we introduced infinite families of good ABC triples, generalized known results, and showed that there are infinitely many good isogeny classes of elliptic curves with a 12-isogeny.

ABC Conjecture

The ABC Conjecture states the following: For $\varepsilon > 0$, there exist only finitely many triples (a, b, c) of coprime positive integers with $a + b = c$ such that

$$c > \mathrm{rad}(abc)^{1+\varepsilon}$$

Good ABC Triples

An **abc triple**, is a triple of positive integers, (a, b, c), such that $a + b = c$, $a < b < c$, and $\gcd(a, b) = 1$. An abc triple is defined to be **good** if

$$\mathrm{rad}(abc) < c$$

where the radical of abc, denoted by $\mathrm{rad}(abc)$, are the product of the distinct primes dividing abc.

a	b	c	rad(abc)
1	8	9	6
5	27	32	30
1	48	49	42
1	63	64	30
1	80	81	30
32	49	81	42
4	121	125	110
3	125	128	30

Figure: The table below lists all good ABC triples (a, b, c) with $a < b < c < 200$.

While good abc triple are rare, there are infinitely many good abc triples which demonstrates the need for the ϵ in the ABC Conjecture.

Specifically, the following two constructions show that there are infinitely many good abc triples.
(1) For each odd prime p, the following abc triple is good: $(1, 2^{p(p-1)}-1, 2^{p(p-1)})$ (Granville,Tucker,2002).
(2) For p an odd prime and k a positive integer, the abc triple $(1, p^{(p-1)k} - 1, p^{(p-1)k})$ (Barrios, 2020).
Our first result generalizes these two constructions:

Theorem(A-S,H)

For every positive integer k, the following are good ABC triples:

1. $(1, n^{(n-1)k} - 1, n^{(n-1)k})$ if n is a positive odd integer
2. $(1, n^{(n+1)k}, n^{(n+1)k} + 1)$ if n is an even integer
3. $(1, n^{(n+1)k} - 1, n^{(n+1)k})$ if n is an odd positive integer and either $2|(n + 1)$ or $2|k$
4. $(1, n^{\varphi(m)k} - 1, n^{\varphi(m)k})$ if m is a positive integer such that $\gcd(m, n) = 1$, and $\frac{m}{\mathrm{rad}(m)} > n$
   - $\varphi(m)$ is the number of relatively prime positive integers to m that are less than m

Elliptic Curves

An **Elliptic Curve** over $\mathbb{Q}$ is the set of rational numbers (x, y) that satisfy the equation

$$y^2 = x^3 + Ax + B$$

together with a point "at infinity" denoted $\mathcal{O}$, where $A, B \in \mathbb{Q}$ satisfy $4A^3 + 27B^2 \neq 0$. There is a natural group structure of the points on an elliptic curve where $\mathcal{O}$ is the identity. We say that E_1 is **$\mathbb{Q}$-isomorphic** to E_2 if there exists $\phi : E_1 \to E_2$ with the property that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ and ϕ is defined as

$$\phi(x, y) = (u^2x + r, u^3y + u^2sx + w)$$

where $u, r, s, w \in \mathbb{Q}$ and $u \neq 0$. Let E be a rational elliptic curve. A **global minimal model** for E is a Weierstrass model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

such that each $a_j \in \mathbb{Z}$ and the absolute value of the discriminant, $|\Delta|$, is minimal over all $\mathbb{Q}$-isomorphic elliptic curves to E. The **minimal discriminant** of E, denoted $\Delta_E^{\min}$, is the discriminant of a global minimal model. Moreover, we have the identity $1728\Delta_E^{\min} = c_4^3 - c_6^2$. If the $\gcd(c_4, \Delta_E^{\min}) = 1$, then we say that E is a **semistable** elliptic curve. If E is a semistable elliptic curve, then the **conductor**, N_E of E satisfies $N_E = \mathrm{rad}(\Delta_E^{\min})$.

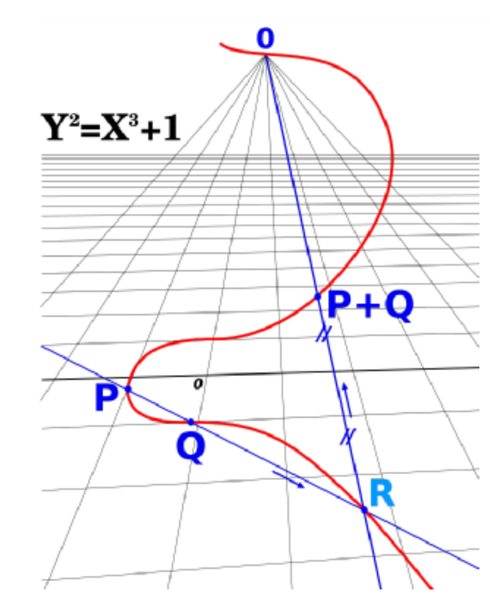

Figure: The Group Law on an Elliptic Curve

Good Elliptic Curves

The **Modified Szpiro Conjecture** states that for any given $\epsilon > 0$, there are finitely many elliptic curves E over $\mathbb{Q}$ (up to isomorphism) such that

$$N_E^{6+\epsilon} < \max\{|c_4|^3, c_6^2\}$$

where c_4,c_6 are associated to a minimal model of E. An elliptic curve is defined to be **good** if

$$N_E^6 < \max\{|c_4|^3, c_6^2\}$$

Isogenies and Isogeny Classes

An **isogeny** $\pi : E \to E'$ between elliptic curves is a nonzero surjective group homomorphism with finite kernel. An **n-isogeny** is an isogeny such that

$$\ker(\pi) \cong \mathbb{Z}/n\mathbb{Z}.$$

The **isogeny class (over Q)** of an elliptic curve $E/\mathbb{Q}$ is the set of all isomorphism classes of elliptic curves defined over $\mathbb{Q}$ that are isogenous to $E/\mathbb{Q}$.

Our Project

Elliptic curves with a non-trivial n-isogeny can be parameterized in terms of a family of n-isogenous, non-isomorphic curves $F_{n,i}(a, b, d)$ for some coprime integers a, b and some square-free integer d. In particular, if E is an elliptic curve over $\mathbb{Q}$ that admits a non-trivial n-isogeny, then its isogeny class is given by $\{F_{n,i}(a, b, d)\}$.
Our research is motivated by the following question: are there infinitely many isogeny classes with the property that each of its members is a good elliptic curve? We call these isogeny classes **good isogeny classes**. The following result shows that there are infinitely many good isogeny classes.

Theorem(A-S,H)

Let (a, b, c) be a good ABC triple such that $b \equiv 0 \mod 6$, then the isogeny class of

$$F_{12,i}(a, b)$$

is good whenever $\frac{b}{a} > 25.4928$

Good Elliptic Curves from Good ABC Triples

Consider the family of good abc triples $(1, n^{(n+1)k}, n^{(n+1)k} + 1)$. If we choose $n = 6$, then $\frac{b}{a} = n^{(n+1)k} = 6^{7k}$ satisfies the properties for our theorem for $k \geq 1$ and therefore produces infinitely many good isogeny class.

Acknowledgements

We would like to thank:

- Pomona College for making PRiME 2022 possible
- Dr. Alex Barrios, Summer Soller, and all PRiME 2022 staff for their guidance and expertise throughout this experience.

This material is based on work supported by the National Science Foundation (DMS-2113782).