A Look at the ABC Conjecture via Elliptic Curves

Nicole Cleary
Brittany DiPietro
Alexander Hill
Gerard D.Koffi
Beihua Yan

Abstract

We study the connection between elliptic curves and ABC triples. Two important results are proved. The first gives a method for finding new ABC triples. The second result states conditions under which the power of the new ABC triple increases or decreases. Finally, we present two algorithms stemming from these two results.

1 Introduction

The ABC conjecture is a central open problem in number theory. It was formulated in 1985 by Joseph Oesterlé and David Masser, who worked separately but eventually proposed equivalent conjectures. Like many other problems in number theory, the ABC conjecture can be stated in relatively simple, understandable terms. However, there are several profound implications of the ABC conjecture. Fermat's Last Theorem is one such implication which we will explore in the second section of this paper.

1.1 Statement of The ABC Conjecture

Before stating the ABC conjecture, we define a few terms that are used frequently throughout this paper.

Definition 1.1.1 The **radical** of a positive integer n, denoted **rad(n)**, is defined as the product of the distinct prime factors of n. That is,

$$rad(n) = \prod_{p|n} p \quad \text{where } p \text{ is prime.}$$

Example 1.1.2 Let $n = 72 = 2^3 \cdot 3^2$. Then $rad(n) = rad(72) = rad(2^3 \cdot 3^2) = 2 \cdot 3 = 6$.

Definition 1.1.3 Let $A, B, C \in \mathbb{Z}$. A triple (A, B, C) is called an **ABC triple** if $A + B = C$ and $\gcd(A, B, C) = 1$.

Note: We can rearrange any given ABC triple so that $A, B, C > 0$. Hence, we assume in this paper that the ABC triples are positive.

Example 1.1.4 By taking the absolute value of each element of $(3, -7, 4)$, we can rearrange it as $(3, 4, 7)$ to be an ABC triple.

Remark 1.1.5 Since $A + B = C$, exactly one of the A, B or C must be divisible by 2. Hence, The product ABC is divisible by 2.

Definition 1.1.6 Let (A, B, C) be an ABC triple. Then $P(A, B, C) = \frac{\log(C)}{\log(rad(ABC))}$ is called the **power**.

Example 1.1.7 If $A = 3, B = 4, C = 7$, then $rad(3 \cdot 2^2 \cdot 7) = 3 \cdot 2 \cdot 7 = 42$ and $P(3, 4, 7) = \frac{\log(7)}{\log(42)} \approx 0.520$.

Note that most of the time, $P(A, B, C)$ is less than 1. For our research, we focus on the ABC triples with power greater than 1.

Example 1.1.8 If $A = 1, B = 8$, and $C = A + B = 9$, then $rad(1 \cdot 8 \cdot 9) = rad(8 \cdot 9) = rad(2^3 \cdot 3^2) = 2 \cdot 3 = 6$ and $P(1, 8, 9) = \frac{\log(9)}{\log(6)} \approx 1.226$.

ABC triples with $P(A, B, C) > 1$ are considered **exceptional** . The highest power found thus far is 1.6299 and it corresponds to the ABC triple $A = 2, B = 3^{10} \cdot 109$, and $C = 23^5$. This triple was found by Eric Reyssat in 1987.

Joseph Oesterlé, one of the men that posed the ABC conjecture, was motivated by the Szpiro Conjecture, which encompasses many ideas of elliptic curves. The following is the first version of the ABC conjecture posed by Oesterlé.

Conjecture 1.1.9 (Oesterlé,[8]) For any $\varepsilon > 0$, there exists only finitely many non-trivial ABC triples such that $P(A, B, C) > 1 + \varepsilon$.

A little later, David Masser developed the ABC conjecture while working with Mason's Theorem, which examines the degree of a polynomial and the radical of a polynomial. David Masser proposed this conjecture by taking Mason's Theorem and converting the polynomials into integers. The following is the equivalent version of the ABC conjecture presented by Masser.

Conjecture 1.1.10 (Masser,[8]) For every $\varepsilon > 0$, there exist only finitely many non-trivial ABC triples such that $C \leq C(\varepsilon) \cdot rad(ABC)^{1+\varepsilon}$, where $C(\varepsilon)$ is a constant that depends only on ε.

The ABC conjecture proves to be one that requires more attention than is available during this seven week research program. As a result, we decide to use our resources to further explore the conjecture. In this paper, we focus on Oesterlé's version of the ABC conjecture and its connection with elliptic curves. Through our examination of elliptic curves, we devise a method that leads to the discovery of ABC triples of powers 1.3428 and 1.4567. We also discover new ABC triples with significantly high merits of 23.710 and 23.68.
We believe that with further research, additional high powered triples can be constructed using our methods.

2 Fermat's Last Theorem and the ABC Conjecture

2.1 Fermat's Last Theorem

Fermat's Last Theorem was first posed in 1637 by Pierre de Fermat. By looking at the method used to prove Fermat's Last Theorem in 1994, we hope to gain insight to the ABC conjecture. We now explore a brief overview of the proof of the theorem to help demonstrate why an elliptic curve approach may yield results in the ABC conjecture.

Theorem 2.1.1 (Fermat's Last Theorem) For $a, b, c \in \mathbb{Z}^+$, the equation $a^n + b^n = c^n$ has no nonzero solutions for any integer $n > 2$.

Fermat did not provide a proof for all $n > 2$, but he did prove the case when $n = 4$ and Euler was able to reduce to the case where n is an odd prime. After over 300 years, there was still no complete proof of Fermat's Last Theorem. In 1984, Gerhard Frey proposed another way of looking at the problem using the theory of elliptic curves.

Definition 2.1.2 An **elliptic curve** E is a geometric object which can be modeled by an equation of the form $E : y^2 = x^3 + Ax + B$, where A and B are rational numbers such that $\Delta = -16(4A^3 + 27B^2) \neq 0$.

Remark 2.1.3 $\Delta = -16(4A^3 + 27B^2) \neq 0$ is called the **discriminant** of the equation $E : y^2 = x^3 + Ax + B$.

Gerhard Frey looked at an elliptic curve of the form $E : y^2 = x(x - a^p)(x + b^p)$, where p is an odd prime. Note that a and b in this equation correspond to Fermat's equation $a^n + b^n = c^n$. Gerhard Frey believed that if Fermat's equation has a solution for $p \geq 5$, then this curve would have such strange properties that it cannot exist. Frey's curve led to the proof of Fermat's Last Theorem in 1994 by Andrew Wiles.

2.2 Asymptotic Fermat's Last Theorem

The motivation for our main approach to the ABC conjecture comes mostly from the proof of Fermat's Last Theorem. As we demonstrate, the ABC conjecture implies the asymptotic case of Fermat's Last Theorem. Though Fermat's Last Theorem took over 300 years to prove, the asymptotic case can be deduced by assuming the ABC conjecture. The asymptotic case of Fermat's Last Theorem states that there are only finitely many solutions to the equation $a^n + b^n = c^n$ for $n > 3$.

Proposition 2.2.1 The ABC conjecture implies the asymptotic case of Fermat's Last Theorem.

Proof. Consider the solutions to $a^n + b^n = c^n$ for $n > 3$ and $a, b, c \in \mathbb{Z}^+$ with $\gcd(a, b, c) = 1$. We investigate the power of these solutions:

$$\begin{aligned} P(a^n, b^n, c^n) &= \frac{\log(c^n)}{\log(rad(a^n b^n c^n))} \\ &= \frac{n\log(c)}{\log(rad(abc))} \\ &\geq \frac{n\log(c)}{\log(rad(a)\cdot rad(b)\cdot rad(c))} \\ &> \frac{n\log(c)}{\log(c^3)} \\ &> \frac{n\log(c)}{3\log(c)} = \frac{n}{3}. \end{aligned}$$

Let $A = a^n, B = b^n$ and $C = c^n$. We have that $P(A, B, C) > \frac{n}{3} > 1 + \varepsilon$. Now, by assuming the ABC conjecture, which states that there are only finitely many ABC triples with $P(A, B, C) > 1 + \varepsilon$, we can then conclude that there are only finitely many n for which Fermat's equation $a^n + b^n = c^n$ holds true. □

By examining the proof of Fermat's Last Theorem and the asymptotic case of Fermat's Last Theorem, we develop some ideas on how to approach the ABC conjecture. It seems that examination through elliptic curves may be the most rewarding approach, and so we take a computational approach via elliptic curves.

3 Elliptic Curves

There are many advantages in looking at elliptic curves. The algebraic group structure of elliptic curves can be used to implement new algorithms to find new ABC triples. Below, we state a few theorems about the group structure of elliptic curves. For more details on elliptic curves see [6].

3.1 Group Structure of Elliptic Curves

Recall that an elliptic curve E is a geometric object which can be modeled by an equation of the form $E : y^2 = x^3 + Ax + B$, where A and B are rational numbers such that $\Delta = -16(4A^3 + 27B^2) \neq 0$.

Let $E(\mathbb{Q})$ be the set of rational points on an elliptic curve E with the point at infinity. We define a binary operation $\oplus$ on $E(\mathbb{Q})$ making the ordered pair $(E(\mathbb{Q}), \oplus)$ an abelian group. In 1923, Mordell proved that $E(\mathbb{Q})$ is finitely generated.

Theorem 3.1.1 (Mordell,[5]) If E is an elliptic curve over $\mathbb{Q}$, then the abelian group $E(\mathbb{Q})$ is finitely generated. Furthermore, there exists a finite group $E(\mathbb{Q})_{tors}$ and a nonnegative integer r such that $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$.

The set $E(\mathbb{Q})_{tors}$ is the collection of points with finite order; it is called the torsion subgroup of E. The nonnegative integer r is called the Mordell-Weil rank of E. In 1977, Barry Mazur completely classified the structure of torsion subgroups of elliptic curves.

Theorem 3.1.2 (Mazur,[4]) If E is an elliptic curve over $\mathbb{Q}$, then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following 15 groups:

(i) Z_n, with $1 \leq n \leq 10$ or $n = 12$.

(ii) $Z_2 \times Z_{2m}$, with $1 \leq m \leq 4$.

In this paper, we focus on the elliptic curves with torsion subgroup $Z_2 \times Z_8$.

3.2 Isogeny and Frey Curves

A special family of elliptic curves is of interest in our research; these curves are called Frey curves, after the German mathematician Gerhard Frey. A Frey curve is defined by the equation $E : y^2 = x(x - A)(x + B)$, where A and B are coprime integers. To a given ABC triple (A, B, C), we associate the Frey curve $E_{(A,B,C)} : y^2 = x(x - A)(x + B)$.

Definition 3.2.1 Let E and E' be two elliptic curves over the field $\mathbb{Q}$. We say that a group homomorphism $\varphi : E \to E'$ over $\mathbb{Q}$ is an **m-isogeny** if the kernel of φ has order m.

For our research, we focus on the case where $m = 2$.

Remark 3.2.2 If $\varphi : E \to E'$ is an isogeny of elliptic curves, then there exists another isogeny $\widehat{\varphi} : E' \to E$ such that $\widehat{\varphi} \circ \varphi$ and $\varphi \circ \widehat{\varphi}$ are multiplication by 2 on E and E', respectively. We call $\widehat{\varphi}$ the **dual isogeny** to φ.

Theorem 3.2.3 Let α and β be rational numbers such that $\beta(\alpha^2 - 4\beta) \neq 0$ and let $E : y^2 = x^3 + \alpha x^2 + \beta x$ and $E' : y^2 = x^3 - 2\alpha x^2 + (\alpha^2 - 4\beta)x$ be two elliptic curves. Then there is a 2-isogeny from E to E'.

For a proof of Theorem 3.2.3 see [3] and [6]. We use this theorem to generate new ABC triples and refer to the application of the 2-isogeny map as the **isogeny method.**

3.3 "Isogenous" Triples

Definition 3.3.1 An ABC triple (A, B, C) is said to be **2-isogenous** to another ABC triple (A', B', C') if there exists a 2-isogeny between the Frey curves $E_{(A,B,C)}$ and $E_{(B',A',C')}$.

The following lemma is the basis of our main algorithm to find new ABC triples.

Lemma 3.3.2 Let (A, B, C) be an ABC triple with A and C both being squares; that is, $A = a^2$ and $C = c^2$ where $a, c \in \mathbb{Z}^+$. Then (A, B, C) is 2-isogenous to $(A', B', C') = ((c - a)^2, 4ac, (c + a)^2)$.

Proof. Taking the ABC triple (A, B, C), its associated Frey curve is given by $E_{(A,B,C)} : y^2 = x(x - A)(x + B)$. Making the substitution $x = X + A$, we can model $E_{(A,B,C)}$ by

$$\begin{aligned} y^2 &= X(X + A)(X + C) \\ &= X^3 + (A + C)X^2 + (AC)X. \end{aligned}$$

By Theorem 3.2.3, where $\alpha = A + C$ and $\beta = AC$, There is a 2-isogeny from $E_{(A,B,C)}$ to the elliptic curve $E'_{(A,B,C)} : y^2 = X^2 - 2(A + C)X^2 + (C - A)X$. Substituting $A = a^2$ and $C = c^2$, we have

$$\begin{aligned} E'_{(A,B,C)} : y^2 &= X^3 - 2(c^2 + a^2)X^2 + (c^2 - a^2)X \\ &= X(X - (c - a)^2)(X - (c + a)^2). \end{aligned}$$

Then, by making the substitution $X = x + (c-a)^2$, we have

$$\begin{aligned} y^2 &= x(x + (c-a)^2)(x - 4ac) \\ &= x(x - B')(x + A'). \end{aligned}$$

So that $E'_{(A,B,C)}$ is the Frey curve associated to the triple

$$(B', A', C') = (4ac, (c-a)^2, (c+a)^2).$$

This is the same triple as

$$(A', B', C') = ((c-a)^2, 4ac, (c+a)^2) \tag{1}$$

□

We prove later that (1) is an ABC triple.

4 The Hunt for Exceptional Triples

In this section, we present some specific families of ABC triples which allow us to use the isogeny method.

4.1 Pythagoreans Triples

Pythagorean triples are widely known and commonly used in mathematics. They are a set of integer triples (a, b, c) that satisfy a special case of Fermat's Last Theorem $(n = 2)$ $a^2 + b^2 = c^2$, where $abc \neq 0$. See [7] for more about Pythagorean triples. A Pythagorean triple is said to be **primitive** if $\gcd(a, b, c) = 1$.

Example 4.1.1 $(a, b, c) = (3, 4, 5)$ is a primitive Pythagorean triple: $3^2 + 4^2 = 9 + 16 = 25 = 5^2$.

In this paper, we focus on the primitive Pythagorean triples because they are 2-isogenous and can generate new set of ABC triples.

Example 4.1.2 Consider the Pythagorean triple $(A, B, C) = (9, 16, 25)$. Since B and C are squares, by Lemma 3.1, $(9, 16, 25)$ is 2-isogenous to the triple $(A', B', C') = ((5-4)^2, 4 \cdot 5 \cdot 4, (5+4)^2) = (1, 80, 81)$.
Note that $rad(9 \cdot 16 \cdot 25) = rad(3^2 \cdot 2^4 \cdot 5^2) = 30 = rad(1 \cdot 80 \cdot 81) = rad(2^4 \cdot 5 \cdot 3^4)$.

4.2 Getting Good Triples

We now have a more efficient computational approach for finding exceptional triples. Before discussing the significant of these triples, we present the following theorem that results from the isogeny method.

Theorem 4.2.1 Suppose that we have an ABC triple of the form $(A, B, C) = (a^2, B, c^2)$. The new triple given by

$$(A', B', C') = \left(\tfrac{(c-a)^2}{d}, \tfrac{4ac}{d}, \tfrac{(c+a)^2}{d} \right),$$

where $d = \gcd((c-a)^2, 4ac, (c+a)^2)$ is such that the following three statements hold:

(1) (A', B', C') is an ABC triple.

(2) $rad(A'B'C') = rad(ABC)$.

(3) There is a 2-isogeny mapping the associated elliptic curve $E_{(A,B,C)}$ to $E_{(B',A',C')}$.

To prove Theorem 4.2.1, we first present the following lemma.

Lemma 4.2.2 Let (A, B, C) be an ABC triple with $A = a^2$ and $C = c^2$ for some $a, c \in \mathbb{N}$. If $d = \gcd((c-a)^2, 4ac, (c+a)^2)$, then

$$d = \begin{cases} 1, & \text{if } 2 \mid ac \\ 4, & \text{if } 2 \nmid ac. \end{cases}$$

Proof. Suppose that p is an odd prime and p divides d, then p must divide $(c-a)^2, 4ac$, and $(c+a)^2$. Note that it is sufficient to say that p divides $(c-a)^2$ and $4ac$, since $(c+a)^2$ is the sum of the other two. Thus, p divides $(c-a)$ and $p \mid ac$. Since p is an odd prime, it cannot divide 4, so p must divide ac. From the hypothesis of the theorem, $(A, B, C) = (a^2, B, c^2)$ is an ABC triple, hence, $\gcd(a, c) = 1$. For p to divide ac, p must divide either a or c. Without lost of generality, we can say that p divides a. Then since p divides $(c-a)$ and p divides a, p must divide $((c-a)+a)$; that is, p divides c. This contradicts $\gcd(a, c) = 1$. Thus, 2 divides d or $d = 1$. Next, we show that if 2 does not divide ac, d must be 4. Suppose 2 divides d, then 2 divides $(c-a)^2$. Note that if 2 divides $(c-a)^2$, then 2 divides $(c-a)$. Since 2 divides $(c-a)^2$ and 2 divides $4ac$, but 2 does not divide ac, then we have that 2 divides 4. Thus, $d = 4$. Therefore, we have

$$d = \begin{cases} 1, & \text{if } 2 \mid ac \\ 4, & \text{if } 2 \nmid ac. \end{cases}$$

□

Proof of Theorem 4.2.1.

Part 1: To prove that (A', B', C') is an ABC triple, we show that $A' + B' = C'$ and $\gcd(A', B', C') = 1$. Since $A' = \frac{(c-a)^2}{d}$ and $B' = \frac{4ac}{d}$, we have that

$$A' + B' = \tfrac{(c-a)^2+4ac}{d} = \tfrac{c^2-2ac+a^2+4ac}{d} = \tfrac{(c+a)^2}{d} = C'.$$

Since $\gcd((c-a)^2, 4ac, (c+a)^2) = d$, we have that $\gcd\left(\frac{(c-a)^2}{d}, \frac{4ac}{d}, \frac{(c+a)^2}{d}\right) = 1$. Therefore, (A', B', C') is an ABC triple.

Part 2: We show that $rad(A'B'C') = rad(ABC)$. Let $P_n = \{p \mid p \text{ is a prime and } p \text{ divides } n\}$. Since $A = a^2$ and $C = c^2$, then $P_A = P_a$ and $P_C = P_c$. By Lemma 4.2.2, we have two cases: $d = 1$ or $d = 4$.

Case 1: $d = 1$

Note that

$$A'B'C' = (c-a)^2(4ac)(c+a)^2 = (c^2-a^2)(4ac). \qquad (2)$$

By substituting $A = a^2$ and $C = c^2$ into the right-hand side of (2), we have

$$A'B'C' = (C-A)^2(4ac) = (B)^2(4ac) = 4B^2ac.$$

So by applying the definition of radical and using $P_A = P_a$ and $P_C = P_c$, we have

$$\begin{aligned} rad(A'B'C') &= rad(2^2B^2ac) \\ &= rad(2Bac) \\ &= rad(2Ba^2c^2) \\ &= rad(2ABC) \\ &= rad(ABC). \end{aligned}$$

Thus, we conclude that $rad(A'B'C') = rad(ABC)$.

case 2: $d = 4$

Note that for $d = 4$, $rad\,(A'B'C') = rad\left(\frac{(c-a)^2}{4}, \frac{4ac}{4}, \frac{(c+a)^2}{4}\right)$. We need to show $rad\left(\frac{(c-a)^2}{4}, \frac{4ac}{4}, \frac{(c+a)^2}{4}\right) = rad((c-a)^2, 4ac, (c+a)^2)$. Since $d = 4 = 2^2$, we only need to show that $2 \in P_{A'B'C'}$. Since $(A'B'C')$ is an ABC triple, by Remark 1.1.2, we know that 2 always divides $A'B'C'$. Therefore, 2 must be an element of $P_{A'B'C'}$. Hence,

$$\begin{aligned} rad(A'B'C') &= rad\left(\frac{(c-a)^2}{4}, \frac{4ac}{4}, \frac{(c+a)^2}{4}\right) \\ &= rad((c-a)^2, 4ac, (c+a)^2) \\ &= rad(ABC). \end{aligned}$$

This completes the proof of part 2.

Part 3: Given the Frey curves $E_{(A,B,C)} : y^2 = x(x-A)(x+B)$ and $E_{(B',A',C')} : y^2 = x(x-B')(x+A')$, the 2-isogeny φ

$$\varphi : E_{(A,B,C)} \to E_{(B',A',C')},$$

is given by $\varphi(x,y) = \left(\frac{B^2}{4d(x-A)} + \frac{x-3A-2C}{4d} - A', \frac{y}{8d^{3/2}}\left(1 - \frac{B^2}{(x-A)^2}\right)\right)$.

The dual isogeny $\hat{\varphi}$

$$\widehat{\varphi} : E_{(B',A',C')} \to E_{(A,B,C)},$$

is given by $\widehat{\varphi}(x,y) = \left(\frac{d(A')^2}{16(x-B')} + \frac{d(x-3B'-2C')}{16} - B, \frac{d^{3/2}y}{64}\left(1 - \frac{(A')^2}{(x-B)^2}\right)\right)$. □

Our research goal is to find more exceptional ABC triples. Given any 2- isogenous ABC triple (A, B, C), we are able to generate a new ABC triple (A', B', C'). The following theorem shows under which condition this new triple has a higher power.

Theorem 4.2.3 Given any 2-isogenous ABC triples (A, B, C) and (A', B', C') satisfying the condition of Theorem 4.2.1., the following statements hold:

(1) If 2 divides ac, then $P(A', B', C') > P(A, B, C)$.

(2) If 2 does not divide ac, then $P(A', B', C') < P(A, B, C)$.

Proof.
Part 1: If 2 divides ac, then by Lemma 4.2.2,

$$C' = \frac{(c+a)^2}{1} = c^2 + 2ac + a^2. \tag{3}$$

Substituting $A = a^2$ and $C = c^2$ into the right-hand side of equation (3), we get $C' = C + 2ac + A > C$, since A, a, c are positive integers. Also, from Part 2 of Theorem 4.2.1, we have that $rad(A'B'C') = rad(ABC)$. Thus, $C' > C$ implies that $\frac{\log(C')}{\log(rad(A'B'C'))} > \frac{\log(C)}{\log(rad(ABC))}$. Therefore, $P(A',B',C') > P(A,B,C)$.

Part 2: If 2 does not divide ac, then, from Lemma 4.2.2, $C' = \frac{(c+a)^2}{4}$. Since $A = a^2$, $C = c^2$ and $C - A > 0$, we see that $C' = \frac{(c+a)^2}{4} = \frac{C}{4} + \frac{2ac}{4} + \frac{A}{4} < \frac{4C}{4} = C$. From Part 2 of Theorem 4.2.1, we have $\frac{\log(C')}{\log(rad(A'B'C'))} < \frac{\log(C)}{\log(rad(ABC))}$. Therefore, $P(A',B',C') < P(A,B,C)$. □

Remark 4.2.4 If we have an ABC triple of the form: $(A,B,C) = (A,b^2,c^2)$, we can apply the involution

$$\begin{gathered}(A,B,C) \mapsto (B,A,C)\\ (a^2,c^2) \mapsto (b^2,c^2).\end{gathered}$$

Then Theorem 4.2.1 and Theorem 4.2.3 are applicable to the triple (A,b^2,c^2).

4.3 A Special Family of ABC Triples

Motivated by several ideas from Edray Goins who parameterized specific families of Frey curves(specifically, those with $E(\mathbb{Q})_{tors} \backsimeq Z_2 \times Z_8$), we are able to develop an algorithm to find new triples with higher power. The following proposition describes the form of the new ABC triples we found.

Proposition 4.3.1 Consider the triple given by

$$\begin{aligned}A &= (2mn)^4\\ B &= (m^2+n^2)^2(m^4-6m^2n^2+n^4)\\ C &= (m^2-n^2)^4,\end{aligned}$$

where m,n are integers, such that $\gcd(m,n) = 1$ and $0 < m < (\sqrt{2}-1)n$. This is an ABC triple and is 2-isogenous to

$$(A',B',C') = \left(\frac{(c-a)^2}{d}, \frac{4ac}{d}, \frac{(c+a)^2}{d}\right),$$

where $d = \gcd((c-a)^2, 4ac, (c+a)^2)$.

Note: For B to be a positive integer, the condition $0 < m < (\sqrt{2}-1)n$ is necessary.

To prove Proposition 4.3.1, we need the following Lemma.

Lemma 4.3.2 Let A, B, C be as in Proposition 4.3.1. Then $\gcd(A, B, C) = 2^k$, where $k \geq 0$.

Proof. We prove the Lemma by contradiction. Suppose that p is an odd prime that divides $\gcd(A, B, C)$, then p divides $\gcd(A, C)$. Therefore, p divides C and p divides A. In other words, $p \mid (m^2 - n^2)^4$ and $p \mid (2mn)^4$. Thus, p divides $(m^2 - n^2)$ and p divides 2 or p divides m or p divides n. But $p \neq 2$, so $p \mid m$ or $p \mid n$. Without loss of generality, we assume that p divides n and p divides $(m^2 - n^2)$. Then p divides n^2. Thus, p divides $((m^2 - n^2) + n^2)$ which implies that p divides m. But if p divides m and n, then p divides $\gcd(m, n)$. Since $\gcd(m, n) = 1$, we have a contradiction. Therefore $\gcd(A, B, C) = 2^k$, where $k \geq 0$. □

Proof of Proposition 4.3.1. We show that the triple (A, B, C) satisfies the definition of an ABC triple. We have

$$\begin{aligned}
A + B &= (2mn)^4 + (m^2 + n^2)^2(m^4 - 6m^2n^2 + n^4) \\
&= 16m^4n^4 + (m^4 + 2m^2n^2 + n^4)(m^4 - 6m^2n^2 + n^4) \\
&= m^8 - 4m^6n^2 + 6m^4n^4 - 4m^2n^6 + n^8 \\
&= (m^2 - n^2)^4 \\
&= C.
\end{aligned}$$

To show that $\gcd(A, B, C) = 1$, we consider the following two cases.

Case 1: Exactly one of m, n is odd. Then $2 \mid mn$ and thus 2 divides $(2mn)^4$, but 2 does not divide $(m^2 + n^2)^2(m^4 - 6m^2n^2 + n^4)$ and $(m^2 - n^2)^4$. Therefore, $\gcd(A, B, C) = 1$.

Case 2: Both m, n are odd. Then 2 does not divide mn and thus, 2 divides $(m^2 - n^2)^4, (m^2 + n^2)^2(m^4 - 6m^2n^2 + n^4)$, and $2 \mid (2mn)^4$. Since 2 divides $(2mn)^4$ but not mn, $\gcd(A, B, C) = 2^4 = 16$. In this case, we simply divide A, B, and C by 16 to get an ABC triple.

This completes the proof of (A, B, C) being an ABC triple.

Now, we show that the ABC triple (A, B, C) is 2-isogenous to $(A', B', C') = \left(\frac{(c-a)^2}{d}, \frac{4ac}{d}, \frac{(c+a)^2}{d}\right)$. We write $(A, B, C) = (a^2, B, c^2)$, where $a = (2mn)^2$ and $c = (m^2 - n^2)^2$. By Theorem 4.2.1, we are done. □

The ABC triples of Proposition 4.3.1 are important because the new ABC triple (A', B', C') is also 2-isogenous to another ABC triple (A'', B'', C''). This follows from Theorem 4.2.1. Hence, using part 1 of Theorem 4.2.3 and Remark 4.2.4, we have that the ABC triple given by

$$\begin{aligned} A'' &= (c' - b')^2 \\ B'' &= 4b'c' \\ C'' &= (c' + b')^2, \end{aligned}$$

where $(b')^2 = B'$ and $(c')^2 = C'$, has a power greater than both (A', B', C') and (A, B, C).

5 Computation of ABC Triples

In this section, we discuss algorithms that we use, which are based on certain ABC triples we discussed in previous theorems and the database from the ABC@home project.

5.1 New Results Using ABC@Home Database

The ABC@home project (see [1]) is a worldwide, public project started in 2006 at the University of California Berkeley by Hendrik Willem Lenstra, Jr. It is organized by linking computers worldwide using the parallel processor Berkeley Open Infrastructure for Network Computing(BOINC). The ultimate goal of the project is to find as many ABC triples as possible and use possible patterns of the triples to gain some insight about the ABC conjecture. ABC@home publishes all of their data on their website (other than their actual code for finding new ABC triples) for public use.

ABC@home had found $7,432,345$ ABC triples with power greater than 1.0 at the moment we downloaded the database. By using the list of these published triples, we were able to sort and search through the list to find ABC triples that fit the conditions of the transformations that we have previously constructed. In detail, using the ABC@home database, we took an ABC triple from their database and then created a new ABC triple with higher power that has not yet been found by ABC@home project.

Below is the algorithm that we used for this approach.

Step 1: Sort through the published ABC@home list of triples and eliminate all of the triples whose C values are not a perfect square.

To check if C is a perfect square, we write a function:
Take an integer C.
Compute the prime factorization of C.

Consider the multiplicities of each of the prime factors of C. In order for C to be a square, all of its prime factors must have an even multiplicity. If the multiplicity of a prime factor is odd, it is equivalent to $1 \bmod 2$. If the multiplicity of a prime is even, the multiplicity is equivalent to $0 \bmod 2$. We then add one to each of these integers $\bmod 2$ and take the product.

If the product of the new multiplicities is equal to $1 \bmod 2$, then C is a square.

If the product of the new multiplicities is equal to $0 \bmod 2$, then C is not a square and we will not use those ABC triples. This first test narrows the list of ABC triples down to 803851.

Step 2:. We now take the list of 803851 ABC triples with C being a square and then separate the data into two cases: C is even and C is odd. There are 211347 cases where C is even and 592504 where C is odd.

Step 3: In the case where C is even, If A is a square (using the same methods used to test C) and A is even, then set

$$\begin{aligned} a &= \sqrt{A} \\ c &= \sqrt{C} \\ A' &= (c-a)^2 \\ C' &= (c+a)^2 \\ B' &= C' - A' \end{aligned}$$

If B is an even perfect square, then A cannot be even or else A, B, C would not be relatively prime. We use a similar transformation but simply use B for the new A value:

$$\begin{aligned} a &= \sqrt{B} \\ c &= \sqrt{C} \\ A' &= (c-a)^2 \\ C' &= (c+a)^2 \\ B' &= C' - A' \end{aligned}$$

We output 75531 ABC triples formed by A', B', C'.

Step 4: We now consider the case where C is odd. We perform the same algorithm as stated in step 3, only we want A to be a perfect square and even or B to be a perfect square and even. We output 67067 ABC triples formed by $A', B'C'$ in this case.

Step 5:. In steps 3 and 4, we perform the isogeny trick to get a higher power ABC triple. From the new A', B', C' it is possible that B' is a perfect square and so we will be able to create isogenous triples of even higher power. If B' is a square, we create another ABC triple, call them A'', B'', and C'', where

$$\begin{aligned} c &= \sqrt{C'} \\ b &= \sqrt{B'} \\ A'' &= (c-b)^2 \\ C'' &= (c+b)^2 \\ B'' &= C'' - A'' \end{aligned}$$

Step 6:. Take results produced from steps 3, 4 and 5 and compute the power for all of these ABC triples.
We mainly explored ABC triples with C values greater than 10^{18} because ABC@home has not found any C values bigger than 10^{18} yet. We found many interesting results from this method. Though we did not discover any *exceptional* triples with this method, we did find four ABC triples with power greater than 1.3 which ABC@home has yet to find.

Coming soon to ABC@home:

A	B	C	$Power\ (P)$
19^4	$2^{24}3 \cdot 29^2 61 \cdot 97^3$	$5^{10}107^2 4591^2$	1.3428395975
13^4	$2^{17}3^2 5^5 67^3 3187$	$7^4 283^4 479^2$	1.3346203755
$58\,789^2$	$2^8 7^3 13 \cdot 19^4 127^2 563$	3^{38}	1.3292668591
$80\,363^2$	$2^5 3^2 5^{11} 17 \cdot 19^3 41^2$	$7^2 619^6$	1.3040380428

Table 1: ABC triples found with $P > 1.3$.

5.2 Finding High Merit ABC Triples

As previously noted, the ABC triples are ranked by their power. However, there is another way to order ABC triples; one can also rank them by their merit. The *merit* of an ABC triple is computed using the following formula:

$$Merit(A,B,C) = \Big(P(A,B,C)-1\Big)^2 \Big(\log(rad(ABC)\Big) \log\Big(\log\big(rad(ABC)\big)\Big).$$

The list of the 100 highest merit triples is maintained by Bart de Smit of Leiden University and can be found at [2]. By looking at the list of high merit triples and using the triples with either A or B being squared and C also being a square, we were able to find new ABC triples. We discovered two additional ABC triples by exploiting the original list of high merit triples. In particular, using the ABC triple that is 72nd on the list

$$\begin{aligned}
A &= 17^{10}19^{2}23^{6}\\
B &= 5^{16}13^{4}59^{2}71^{2}89\cdot 1229^{2}5167\\
C &= 2^{4}3^{4}7^{8}587^{6}13183^{2}\\
P(A,B,C) &= 1.3069326041\\
Merit(A,B,C) &= 23.7103957751,
\end{aligned}$$

we used the isogeny method by setting

$$\begin{aligned}
a &= \sqrt{A} = 17^{5}19\cdot 23^{3}\\
c &= \sqrt{C} = 2^{2}3^{2}7^{4}587^{3}13183.
\end{aligned}$$

Note that by theorem 4.2.3, both the power and merit of the triple increased since A and C are perfect squares and C is even. By performing the isogeny transformation, we obtained the new ABC triple given by

$$\begin{aligned}
A' &= (a-c)^{2} = 2^{4}3^{2}7^{4}17^{5}19\cdot 23^{3}587^{3}13183\\
B' &= C' - A' = 13^{8}59^{4}71^{4}89^{2}5167^{2}\\
C' &= (a+c)^{2} = 5^{32}1229^{4}\\
P(A',B',C') &= 1.3069326507\\
Merit(A',B',C') &= 23.7104029680.
\end{aligned}$$

In this case, the merit increased slightly by approximately 0.00000071929. This new triple will replace the original triple and will then become 72nd on the list, Using another ABC triple that is currently 27th on the list

$$\begin{aligned}
A &= 7^{20}11^{24}17^{8}\\
B &= 2^{17}73^{4}163^{2}14449\cdot 17959^{2}939^{2}1810524950039887\\
C &= 3^{34}5^{24}19^{8}71^{2}5347^{2}\\
P(A,B,C) &= 1.2379760043\\
Merit(A,B,C) &= 26.4476190241,
\end{aligned}$$

and by performing the same transformation as above using A and C, we have the new ABC triple

$$\begin{aligned}
&A' = 3^{17}5^{12}7^{10}11^{12}17^{4}19^{4}71 \cdot 5347\\
&B' = 73^{8}14449^{2} \cdot 1810524950039887^{2}\\
&C' = 2^{30}163^{4}17959^{4}53939^{4}\\
&P(A', B', C') = 1.2251884163\\
&Merit(A', B', C') = 23.6816706652.
\end{aligned}$$

Note that since A and C are perfect squares with A and C being both odd, the power and merit of this triple decrease. Nevertheless, the merit, though lower, still ranks 76th on the high merit triple list and is an original product of our research.

5.3 Computing Isogenous Triples

Another algorithm we developed to find new exceptional ABC triples is to parameterize the ABC triples that we obtain when we use the isogeny method. The following pseudocode presents our algorithm. The actual program generates ABC triples with power greater than 1.1 and was written in Mathematica:

```
  Input :  $m, n, q$
           $0 < m < (\sqrt{2} - 1)n$
 Output :  $A, B, C, P, Rad$
     IF    $\gcd(m, n) = 1$
 Define :  $d$
           $d := 2^{4((mn) \mod (2))}$   THEN
           $A := (m^2 + 2mn - n^2)^4/d$
           $B := (16mn(n^2 - m^2)(m^2 + n^2)^2)/d$
           $C := ((m^2 - 2mn - n^2)^4)/d$
           IF   $C > Rad$   THEN
           $P := \log(C)/\log(Rad)$
      IF   $P > 1 + 1/q$   THEN
  Print:   $P, A, B, C$
```

By running the actual code to output 50000 new triples. We were able to get one exceptional ABC triple with power 1.45567, where $m = 1$ and $n = 3$. The corresponding ABC triple is $(1, 2^5 3 \cdot 5^2, 7^4)$. Unfortunately, this ABC triple has already been found. As m and n increased, we found less and less triples of high power. We are running the code to output over 3×10^6 triples that have the possibility of being exceptional ABC triples.

6 Conclusion

Using the isogeny method, we have shown that new exceptional ABC triples can be found. Although our results do not prove or disprove the ABC conjecture, they can be used to write new and more efficient algorithms in the hunt for exceptional ABC triples.

The ABC conjecture offers a new way of expressing Diophantine problems, including the equation of Fermat's Last Theorem. If proven true, it will open the way to solve several problems in number theory such as the Szpiro conjecture, the Hall conjecture, the infinitude of primes satisfying the Wiefrich condition and many more. With all of its implications, the ABC conjecture deserves further computational and theoretical examination.

Acknowledgements

We would like to thank the following agencies for their financial support: The National Security Agency(NSA) and The National Science Foundation(NSF).

We owe our deepest gratitude to Dr. Lakeshia Legette and Jamie Weigandt for their advice, guidance, many suggestions and constant support during this research.

We thank Miami University, its staff and facilities. We thank Dr. Edray Goins and Robert DiPietro for helpful conversations.

Finally, we wish to thank all the 2009 SUMSRI participants for their friendship.

References

[1] ABC@Home Project. http://abcathome,2009, [Online; accessed June-July, 2009].

[2] Bart de Smit. http://www.math.leidenuniv.nl/~desmit/abc/.

[3] Dale Husemöller. *Elliptic curves*, Springer, 2004.

[4] B Mazur. *rational isogenies of prime degree.* Invent. Math. 44(2),129-162, 1978.

[5] L. J Mordell. *Diophantine equations.* Academic Press, London, 1969.

[6] Joseph H. Silverman, John Tate. *Rational Points On Elliptic Curves*, Springer, 1992.

[7] Jörn Steuding. *Diophantine Analysis*, Chapman& Hall/CRC, 2005.

[8] Jeffrey Wheeler. *The abc Conjecture*, Master's thesis, The University of Tennessee Knoxville, 2002.

ncleary@kent.edu, Kent state University-Stark campus, OH.
dipietbr@lewisu.edu, Lewis University, IL.
ahill3@students.morehouse.edu, Morehouse College, GA.
gerard.koffi001@umb.edu, University of Massachusetts Boston, MA.
by9v@virginia.edu, University of Virginia, VA.