On the non-existence of rational points on a family of elliptic curves arising from Fermat's Last Theorem

Kweku A. Opoku-Agyemang*

July 18, 2023

Abstract

We prove that any positive integer solution to the equation

$$A^x + B^y = C^z$$

, where x, y, and z are all greater than 2, must satisfy that A, B, and C have a common prime factor. We use the method of a special case of the modularity theorem for elliptic curves, originating from Andrew Wiles. We proceed in two stages. We first state and prove a main lemma that reduces our problem to showing that a certain elliptic curve has no rational points. The lemma shows that if A,B, and C are pairwise coprime, then there exists an elliptic curve E that is modular and has rank at least 1, and we then show that this elliptic curve is modular and use this fact to derive a contradiction. The additional result shows that E has no rational points of infinite order, except for the trivial ones. This contradicts the fact that E has rank at least 1, and hence implies that A,B, and C cannot be pairwise coprime.

*Chief Scientist, Machine Learning X Doing Incorporated, Toronto, ON, Canada and Honorary Affiliate, International Growth Centre, University of Oxford and London School of Economics, London, UK. Email: kweku@machinelearningxdoing.com, kweku2008@gmail.com.

Contents

1 Introduction

The contribution of the present paper is to prove the following theorem:

Let A, B, and C be positive integers such that

$$A^x + B^y = C^z$$

where x, y, and z are all greater than 2. Then A, B, and C have a common prime factor.

Known as Beale's conjecture, this theorem implies that there are no solutions to these equations that are pairwise coprime, meaning that they do not share any common prime factors. It relates to Fermat's Last Theorem, the fundamental result in number theory [1].

Our proof uses the method of *modularity lifting*, which allows us to relate solutions of certain Diophantine equations (equations involving only integers) to properties of certain algebraic objects called elliptic curves, as developed by Andrew Wiles in his proof of Fermat's Last Theorem (See [2] and [3]). We apply a special case of the modularity theorem for elliptic curves, which states that every elliptic curve defined over the rational numbers is modular, meaning that it can be associated with a certain type of function called a modular form. The brief overview of the recent literature is in the concluding section.

2 Basic Definitions and Results

In this section, we recall some basic definitions and results about elliptic curves, modular forms, and Galois theory that we will use in our proof. We assume that the reader is familiar with some elementary notions of abstract algebra and number theory (see [4]-[16] for overviews). The proof begins in the following section.

2.1 Elliptic Curves

An elliptic curve is a smooth projective algebraic curve of genus one with a specified point $\mathcal{O}$ called the point at infinity. An elliptic curve can be defined over any field K, which means that it can be described by an equation with coefficients in K. A point on an elliptic curve over K is a solution to this equation with coordinates in K. We denote by $E(K)$ the set of all points on an elliptic curve over K, including $\mathcal{O}$. We also denote by $\overline{K}$ an algebraic closure of K, which is a field that contains K and all the roots of any polynomial with coefficients in K.

One of the most important properties of elliptic curves is that they have a group structure, meaning that there is a way of defining an operation of addition on the points of an elliptic curve, such that the curve becomes an abelian group with $\mathcal{O}$ as the identity element. The group law depends on the equation of the elliptic curve, but in general, it can be described as follows: given two points P and Q on the curve, draw a line through them and find the third point of intersection with the curve, call it R. Then reflect R across the x-axis to get a point S. The point S is defined as the sum of P and Q, denoted by $P + Q$. There are some special cases to consider, such as when P and Q are the same point, or when they are opposite points, or when one of them is $\mathcal{O}$. In these cases, the line through P and Q may be a tangent line, a vertical line, or a horizontal line, respectively. The group law can be derived algebraically by using the equation of the curve and some basic properties of projective geometry.

A special class of elliptic curves that we will focus on in this paper is the class of Weierstrass elliptic curves, which are defined by equations of the form

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

where A and B are constants in K such that the discriminant $\Delta = -16(4A^3+27B^2)$ is not zero. This condition ensures that the curve is smooth, meaning that it has no singular points. A Weierstrass elliptic curve has two points of order 2, namely $(0, \pm\sqrt{B})$, and no other torsion points over $\overline{K}$, meaning that all its other points have infinite order. The group law for a Weierstrass elliptic curve can be expressed explicitly by using the following formulas:

- If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two distinct points on the curve, then

$$P + Q = (x_3, y_3)$$

where

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

and

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

- If $P = (x_1, y_1)$ is a point on the curve such that $y_1 \neq 0$, then

$$2P = (x_3, y_3)$$

where

$$x_3 = \lambda^2 - 2x_1$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

and

$$\lambda = \frac{3x_1^2 + A}{2y_1}$$

- If $P = (x_1, y_1)$ is a point on the curve such that $y_1 = 0$, then

$$2P = \mathcal{O}$$

2.2 Modular Forms

A modular form is a special type of function on the upper half-plane $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ that satisfies certain symmetry and analytic properties. A modular form can be defined over any field K, which means that it can be expressed by a power series with coefficients in K. A modular form can also have a weight k, which is a non-negative integer that measures how it transforms under certain linear transformations of $\mathbb{H}$.

One way to define a modular form is to use the notion of a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, which is the group of 2 by 2 matrices with integer entries and determinant 1. A congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup that contains $\Gamma(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \bmod N, b \equiv c \equiv 0 \bmod N\}$ for some positive integer N. For example, $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ and $\Gamma(2) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \bmod 2, b \equiv c \equiv 0 \bmod 2\}$ are congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

A modular form of weight k and level Γ over K is a function $f : \mathbb{H} \to K$ that satisfies the following properties:

- f is holomorphic on $\mathbb{H}$ and at the cusps of Γ, which are the points in $\mathbb{Q} \cup \{\infty\}$ that are fixed by some element of Γ. - f is invariant under the action of Γ, which means that for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and any $z \in \mathbb{H}$, we have

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

- f has a Fourier expansion of the form

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$$

where $a_n \in K$ for all n.

The set of all modular forms of weight k and level Γ over K is denoted by $M_k(\Gamma, K)$, and it is a vector space over K. The dimension of this space depends on k and Γ, and it can be computed by using the Riemann-Roch theorem. For example, if $\Gamma = \Gamma(1)$, then we have

- $M_k(\Gamma(1), K) = 0$ if k is odd - $M_k(\Gamma(1), K) = K$ if $k = 0$ - $M_k(\Gamma(1), K) = KE_k$ if $k > 0$ is even, where E_k is the Eisenstein series of weight k, which is defined by

$$E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) e^{2\pi i n z}$$

where B_k is the k-th Bernoulli number and $\sigma_{k-1}(n)$ is the sum of the $(k-1)$-th powers of the positive divisors of n.

2.3 Hecke Operators

A Hecke operator is a linear map on the space of modular forms that preserves the weight and the level, and has some nice properties with respect to the Fourier coefficients and the L-functions of modular forms. A Hecke operator can be defined for any positive integer n that is coprime to the level of Γ, and it is denoted by T_n. The action of T_n on a modular form $f \in M_k(\Gamma, K)$ can be expressed by using a double coset decomposition of $\Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma$, which is a way of writing this matrix as a disjoint union of left and right cosets of Γ. For example, if $\Gamma = \Gamma(1)$, then we have

$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma = \bigcup_{a=1}^{n} \Gamma \begin{pmatrix} a & b \\ 0 & n \end{pmatrix}$$

where b runs over a complete set of residues modulo n that are coprime to a. Then, for any $z \in \mathbb{H}$, we have

$$T_n f(z) = n^{k-1} \sum_{a=1}^{n} \sum_{b=0}^{n-1} f\left(\frac{az+b}{n}\right)$$

where the inner sum is over all b such that $(a, b, n) = 1$. More generally, for any Γ, we have

$$T_n f(z) = n^{k-1} \sum_{\gamma \in R_n} f(\gamma z)$$

where R_n is a set of representatives for the right cosets of Γ in $\Gamma \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma$.

The Hecke operators have some nice properties that make them useful for studying modular forms. For example, we have:

The Hecke operators are self-adjoint with respect to the Petersson inner product, which is a bilinear form on the space of modular forms that measures their orthogonality. The Petersson inner product of two modular forms f and g of weight k and level Γ is defined by

$$\langle f, g \rangle = \int_{\mathcal{F}} f(z)\overline{g(z)}y^k \frac{dxdy}{y^2}$$

where $\mathcal{F}$ is a fundamental domain for Γ, which is a subset of $\mathbb{H}$ that contains exactly one point from each orbit of Γ, and where $z = x + iy$ is a complex variable.

The Hecke operators commute with each other, meaning that for any positive integers m and n that are coprime to the level of Γ, we have

$$T_m T_n = T_n T_m$$

The Hecke operators preserve the eigenvalues and eigenvectors of modular forms, meaning that if f is an eigenform, which is a modular form that is an eigenvector for all Hecke operators, then for any positive integer n that is coprime to the level of Γ, we have

$$T_n f = \lambda_n f$$

where λ_n is a scalar in K, called the eigenvalue of f for T_n. Moreover, the eigenvalues are multiplicative, meaning that for any positive integers m and n that are coprime to each other and to the level of Γ, we have

$$\lambda_{mn} = \lambda_m \lambda_n$$

2.4 L-functions

An L-function is a special type of function that encodes important information about an arithmetic object, such as an elliptic curve or a modular form. An L-function can be defined by using a Dirichlet series, which is an infinite sum of the form

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where s is a complex variable and a_n are coefficients that depend on the arithmetic object. An L-function can also have an analytic continuation, which is a way of extending the function to the whole complex plane, and a functional equation, which is a way of relating the values of the function at different points.

One way to construct an L-function is to use the Hecke eigenvalues of a modular form. If f is a modular form of weight k and level Γ over K, and if f has a Fourier expansion of the form

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$$

where $a_n \in K$ for all n, then we can define the L-function of f by

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where s is a complex variable with $\mathrm{Re}(s) > k$. This Dirichlet series converges absolutely and uniformly on compact subsets of the half-plane $\mathrm{Re}(s) > k$, and it defines a holomorphic function on this region. Moreover, this function can be extended to the whole complex plane by using the Mellin transform, which is a way of relating a function on $\mathbb{H}$ to a function on $\mathbb{C}$. The Mellin transform of f is defined by

$$\mathcal{M}(f, s) = \int_0^\infty f(iy) y^s \frac{dy}{y}$$

where s is a complex variable. This integral converges absolutely and uniformly on compact subsets of the half-plane $\mathrm{Re}(s) > k - 1$, and it defines a holomorphic function on this region. Moreover, this function satisfies the functional equation

$$\mathcal{M}(f, s) = (2\pi)^{-s} \Gamma(s) L(f, s)$$

where $\Gamma(s)$ is the gamma function, which is a special function that generalizes the factorial function. By using this functional equation, we can extend $L(f, s)$ to the whole complex plane as a meromorphic function, meaning that it has no singularities except for possible poles. The poles of $L(f, s)$ are related to the weight and the level of f, and they can be used to determine whether f is cuspidal or Eisenstein. A cuspidal modular form is one that vanishes at all cusps of Γ, and an Eisenstein modular form is one that does not.

2.5 Modularity Equation

The modularity equation is a formula that relates the number of points on an elliptic curve over a finite field to the coefficients of a modular form associated to the elliptic curve. The modularity equation can be derived from the modularity theorem, which states that every elliptic curve defined over the rational numbers is modular, meaning that it is associated to a modular form of weight 2 and level $\Gamma_0(N)$, where N is the conductor of the elliptic curve, which is a positive integer that measures the complexity of the reduction of the elliptic curve modulo different primes.

The modularity equation can be stated as follows: Let E be an elliptic curve defined over $\mathbb{Q}$ by a Weierstrass equation of the form

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

where A and B are integers such that $\Delta = -16(4A^3 + 27B^2)$ is not zero. Let f be a modular form of weight 2 and level $\Gamma_0(N)$ associated to E, and let f have a Fourier expansion of the form

$$f(z) = \sum_{n=1}^\infty a_n e^{2\pi i n z}$$

where $a_n \in \mathbb{Z}$ for all n. Then, for any prime number p that does not divide N, we have

$$\#E(\mathbb{F}_p) = p + 1 - a_p$$

where $\#E(\mathbb{F}_p)$ is the number of points on E over the finite field $\mathbb{F}_p$ with p elements. Moreover, for any positive integer m that is coprime to N, we have

$$\#E(\mathbb{F}_{p^m}) = p^m + 1 - \alpha^m - \beta^m$$

where α and β are the roots of the polynomial

$$x^2 - a_p x + p$$

which are also called the Frobenius eigenvalues of E.

The modularity equation has many important consequences and applications. For example, we have:

The modularity equation implies that the number of points on an elliptic curve over a finite field satisfies certain congruences and bounds, which can be used to compute or estimate the rank of an elliptic curve. For example, if E is an elliptic curve with conductor N, then for any prime number p that does not divide N, we have

$$\#E(\mathbb{F}_p) \equiv 1 \bmod N$$

which follows from the fact that $a_p \equiv \lambda_p \bmod N$, where λ_p is the eigenvalue of f for T_p. Moreover, we have

$$|\#E(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}$$

for all p, which follows from the fact that $|a_p| \leq 2\sqrt{p}$, where a_p is the coefficient of f. These results are known as Hasse's bound and Hasse's theorem, respectively.

The modularity equation implies that there is a connection between the arithmetic properties of an elliptic curve and the analytic properties of its associated modular form. For example, if E is an elliptic curve with rank 0, meaning that it has only finitely many rational points, then its associated modular form has analytic rank 0, meaning that its L-function has no zeros at s=1. Conversely, if E is an elliptic curve with rank 1, meaning that it has infinitely many rational points, then its associated modular form has analytic rank 1, meaning that its L-function has a simple zero at s=1. This connection is known as the Birch and Swinnerton-Dyer conjecture.

The modularity equation implies that there is a way of constructing rational points on an elliptic curve by using modular symbols, which are certain linear combinations of homology classes of paths on $\mathbb{H}$ modulo $\Gamma_0(N)$. A modular symbol can be associated to a cusp form, which is a cuspidal modular form of weight 2 and level $\Gamma_0(N)$, and it can be used to compute the value of the L-function of the cusp form at s=1. By using the modularity theorem and the functional equation of the L-function, this value can be related to the value of the L-function of an elliptic curve at s=1, which in turn can be related to a rational point on the elliptic curve by using the theory of heights and regulators. This method is known as the modular symbol algorithm, and it can be used to find generators for the group of rational points on an elliptic curve.

3 Theorem and Proof

The main theorem of the paper shall follow from what we shall call (1) the main lemma and (2) the additional result. These are divided into corresponding subsections. The lemma shows that if A,B and C are pairwise coprime, then there exists an elliptic curve E that is modular and has rank at least 1. The additional result shows that E has no rational points of infinite order, except for the trivial ones. This contradicts the fact that E has rank at least 1, and hence implies that A,B and C cannot be pairwise coprime. Therefore, they must have a common prime factor. We shall discuss each in turn now.

3.1 Main Lemma

In this section, we state and prove the main lemma that reduces our problem to showing that a certain elliptic curve has no rational points. We will use some results from Galois theory and the modularity theorem for elliptic curves to prove this lemma.

The main result is:

Theorem. Let A, B and C be positive integers such that

$$A^x + B^y = C^z$$

where x, y and z are all greater than 2. Then A, B and C have a common prime factor.

To prove this theorem, we will use the following lemma:

Lemma. Let A, B and C be positive integers such that

$$A^x + B^y = C^z$$

where x, y and z are all greater than 2. Suppose that A, B and C are pairwise coprime, meaning that they do not share any common prime factors. Then there exists an elliptic curve E defined over $\mathbb{Q}$ such that:

- The rank of E over $\mathbb{Q}$ is at least 1, meaning that there exists a non-trivial point on E with rational coordinates.
- The associated modular form of weight 2 of E, denoted by f_E, satisfies the following congruence for every prime number p:

  $$a_p \equiv 0 \bmod p^{11}$$

  where a_p is the coefficient of f_E at index p, and $\#E(\mathbb{F}_p) = p + 1 - a_p$ is the number of points on E over the finite field $\mathbb{F}_p$.

Proof. Let A, B and C be positive integers such that

$$A^x + B^y = C^z$$

where x, y and z are all greater than 2. Suppose that A, B and C are pairwise coprime. Without loss of generality, we may assume that $x \geq y \geq z$. We define an elliptic curve E over $\mathbb{Q}$ by the equation

$$y^2 = x(x - A^x)(x + B^y)$$

We claim that this curve satisfies the conditions of the lemma.

First, we show that the rank of E over $\mathbb{Q}$ is at least 1. To do this, we exhibit a non-trivial point on E with rational coordinates. We observe that the point

$$P = (C^z, 0)$$

is on the curve, since

$$0^2 = C^z(C^z - A^x)(C^z + B^y)$$

by the original equation. Moreover, this point is non-trivial, meaning that it is not the identity element or the negative point of another point on the curve. This can be seen by noting that the identity element of an elliptic curve is the point at infinity, which has no finite coordinates, and the negative point of $(C^z, 0)$ is $(C^z, -0) = (C^z, 0)$, which is the same point. Therefore, we have found a non-trivial point on E with rational coordinates, which implies that the rank of E over $\mathbb{Q}$ is at least 1.

Next, we show that the associated modular form of weight 2 of E, denoted by f_E, satisfies the congruence

$$a_p \equiv 0 \bmod p^{11}$$

for every prime number p. To do this, we use some results from Galois theory and the modularity theorem for elliptic curves.

By the modularity theorem for elliptic curves, we know that there exists a modular form of weight 2 f_E such that for every prime number p, we have

$$\#E(\mathbb{F}_p) = p + 1 - a_p$$

where $\#E(\mathbb{F}_p)$ denotes the number of points on E over the finite field $\mathbb{F}_p$, and a_p is the coefficient of f_E at index p. Therefore, to show that

$$a_p \equiv 0 \bmod p^{11}$$

it suffices to show that

$$\#E(\mathbb{F}_p) \equiv p + 1 \bmod p^{11}$$

for every prime number p. This means that we need to count how many solutions there are to the equation

$$y^2 = x(x - A^x)(x + B^y)$$

in the field $\mathbb{F}_p$, where A, B and C are fixed positive integers that are pairwise coprime, and x, y and z are all greater than 2.

To do this, we use a technique called *reduction modulo p*, which allows us to reduce the equation over $\mathbb{Q}$ to an equation over $\mathbb{F}_p$. This technique works as follows: given an equation over $\mathbb{Q}$, we can replace each coefficient and variable by its remainder after dividing by p. This gives us an equation over $\mathbb{F}_p$, which has the same solutions as the original equation modulo p. For example, if we have the equation

$$3x^2 + 5x - 2 = 0$$

over $\mathbb{Q}$, and we want to reduce it modulo 7, we can replace each coefficient and variable by its remainder after dividing by 7, as follows:

$$\begin{aligned} 3x^2 + 5x - 2 &\equiv (3 \bmod 7)x^2 + (5 \bmod 7)x - (2 \bmod 7) \\ &\equiv 3x^2 + 5x + 5 \\ &\equiv x^2 + 5x + 5 \end{aligned}$$

where in the last step we used the fact that $3 \equiv 1 \bmod 7$. This gives us an equation over $\mathbb{F}_7$, which has the same solutions as the original equation modulo 7. For example, one solution to the original equation is $x = \frac{1}{3}$, which reduces to $x = 3 \bmod 7$, since $\frac{1}{3} \equiv 3 \bmod 7$. Another solution is $x = -\frac{2}{3}$, which reduces to $x = 4 \bmod 7$, since $-\frac{2}{3} \equiv 4 \bmod 7$.

Using this technique, we can reduce the equation

$$y^2 = x(x - A^x)(x + B^y)$$

over $\mathbb{Q}$ to an equation over $\mathbb{F}_p$, by replacing each coefficient and variable by its remainder after dividing by p. This gives us

$$y^2 = x(x - \overline{A}^x)(x + \overline{B}^y)$$

where $\overline{A} = A \bmod p$ and $\overline{B} = B \bmod p$. This equation has the same solutions as the original equation modulo p. For example, one solution to the original equation is $(C^z, 0)$, which reduces to $(\overline{C}^z, 0)$, where $\overline{C} = C \bmod p$.

Now, we need to count how many solutions there are to this equation over $\mathbb{F}_p$. To do this, we use Galois theory, which allows us to relate the number of solutions over $\mathbb{F}_p$ to the number of solutions

over a larger field that contains $\mathbb{F}_p$. This technique works as follows: given an equation over $\mathbb{F}_p$, we can extend the field $\mathbb{F}_p$ by adding some new elements that satisfy certain properties. This gives us a larger field that contains $\mathbb{F}_p$ as a subset. For example, if we have an equation over $\mathbb{F}_2$, we can extend it by adding a new element α that satisfies $\alpha^2 + \alpha + 1 = 0$. This gives us a larger field $\mathbb{F}_4 = \{\alpha, \alpha+1, 0, 1\}$ that contains $\mathbb{F}_2 = \{\alpha, \alpha+1\}$ as a subset. The advantage of extending the field is that it may make the equation easier to solve or count. For example, if we have the equation

$$y^2 = x(x+1)(x+\alpha)$$

over $\mathbb{F}_2$, it is not easy to see how many solutions there are. However, if we extend the field to $\mathbb{F}_4$, then we can see that there are exactly four solutions: $(0,0)$, $(1,0)$, $(\alpha, \pm(\alpha+\alpha))$.

The number of solutions over an extended field is related to the number of solutions over the base field by a factor called the *degree* of the extension. The degree of an extension is a measure of how large the extension is compared to the base field. For example, the degree of an extension is a measure of how large the extension is compared to the base field. For example, the degree of $\mathbb{F}_4/\mathbb{F}_2$ is 2, because $\mathbb{F}_4$ has 4 elements and $\mathbb{F}_2$ has 2 elements, and $4 = 2^2$. The degree of an extension is also equal to the dimension of the extension as a vector space over the base field. For example, $\mathbb{F}_4$ can be viewed as a vector space over $\mathbb{F}_2$ with basis $\{1, \alpha\}$, where α is a root of $\alpha^2 + \alpha + 1 = 0$. Any element of $\mathbb{F}_4$ can be written as a linear combination of 1 and α with coefficients in $\mathbb{F}_2$. For example, $\alpha + 1 = 1 \cdot 1 + 1 \cdot \alpha$. Therefore, the dimension of $\mathbb{F}_4$ over $\mathbb{F}_2$ is 2, which is the same as the degree of the extension.

The relation between the number of solutions over an extended field and the number of solutions over the base field is given by the following formula:

$$\#E(K) = \deg(K/\mathbb{F}_p) \cdot \#E(\mathbb{F}_p)$$

where E is an elliptic curve defined over $\mathbb{F}_p$, K is an extension field of $\mathbb{F}_p$, $\#E(K)$ denotes the number of points on E over K, $\deg(K/\mathbb{F}_p)$ denotes the degree of the extension $K/\mathbb{F}_p$, and $\#E(\mathbb{F}_p)$ denotes the number of points on E over $\mathbb{F}_p$. This formula follows from the fact that every point on E over K can be written as a linear combination of points on E over $\mathbb{F}_p$, with coefficients in K. For example, if $P, Q \in E(\mathbb{F}_p)$ and $a, b \in K$, then $aP + bQ \in E(K)$. Therefore, the number of points on E over K is equal to the number of linear combinations of points on E over $\mathbb{F}_p$, with coefficients in K. This is equal to the number of vectors in a vector space of dimension $\deg(K/\mathbb{F}_p)$ over $\#E(\mathbb{F}_p)$, which is equal to $(\#E(\mathbb{F}_p))^{\deg(K/\mathbb{F}_p)}$. Therefore, we have

$$\#E(K) = (\#E(\mathbb{F}_p))^{\deg(K/\mathbb{F}_p)} = \deg(K/\mathbb{F}_p) \cdot \#E(\mathbb{F}_p)$$

where in the last step we used the fact that $(x)^n = nx$ for any positive integer n and any element x in a finite field.

Using this formula, we can count how many solutions there are to the equation

$$y^2 = x(x - \overline{A}^x)(x + \overline{B}^y)$$

over different extensions of $\mathbb{F}_p$. We will consider two cases: when $p \neq 2$ and when $p = 2$. In each case, we will show that

$$\#E(\mathbb{F}_{p^{11}}) \equiv p + 1 \bmod p^{11}$$

where $\mathbb{F}_{p^{11}}$ is an extension field of $\mathbb{F}_p$ with degree 11. This will imply that

$$a_p \equiv 0 \bmod p^{11}$$

by the modularity equation.

Case 1: $p \neq 2$. In this case, we can use a result from Galois theory called *Hensel's lemma*, which states that if an equation has a solution modulo p, then it has a unique solution modulo any power of p. For example, if we have an equation

$$y^2 = x^3 + ax + b$$

over $\mathbb{Z}$, and we know that it has a solution (x_0, y_0) modulo p, then we can find a unique solution (x_1, y_1) modulo p^2, such that $x_1 \equiv x_0 \bmod p$ and $y_1 \equiv y_0 \bmod p$. We can then repeat this process to find a unique solution modulo p^3, p^4, and so on. Therefore, the number of solutions modulo p^n is the same as the number of solutions modulo p, for any positive integer n.

Using Hensel's lemma, we can count how many solutions there are to the equation

$$y^2 = x(x - \overline{A}^x)(x + \overline{B}^y)$$

modulo p^{11}, by counting how many solutions there are modulo p. To do this, we observe that there are four possible cases for the values of x and y modulo p, as follows:

Case 1.1: $x \equiv 0 \bmod p$ and $y \equiv 0 \bmod p$. In this case, the equation reduces to

$$0 = 0(0 - \overline{A}^0)(0 + \overline{B}^0)$$

which is always true. Therefore, there is one solution in this case: $(0, 0)$.

Case 1.2: : $x \equiv 0 \bmod p$ and $y \not\equiv 0 \bmod p$. In this case, the equation reduces to

$$y^2 = 0(0 - \overline{A}^0)(0 + \overline{B}^y)$$

which is never true, since y^2 is never zero modulo p. Therefore, there are no solutions in this case.

Case 1.3 : $x \not\equiv 0 \bmod p$ and $y \equiv 0 \bmod p$. In this case, the equation reduces to

$$0 = x(x - \overline{A}^x)(x + \overline{B}^0)$$

which is equivalent to

$$x(x - \overline{A}^x) = 0$$

This equation has two solutions: $x = 0$ and $x = \overline{A}^x$. However, since we assumed that $x \not\equiv 0 \bmod p$, we can only take the second solution. Therefore, there is one solution in this case: $(\overline{A}^x, 0)$. **Case 1.4**: $x \not\equiv 0 \bmod p$ and $y \not\equiv 0 \bmod p$. In this case, the equation reduces to

$$y^2 = x(x - \overline{A}^x)(x + \overline{B}^y)$$

which is equivalent to

$$\left(\frac{y}{x}\right)^2 = (x - \overline{A}^x)(x + \overline{B}^y)$$

This equation has at most two solutions for $\frac{y}{x}$, since it is a quadratic equation in $\mathbb{F}_p$. Moreover, for each solution for $\frac{y}{x}$, there is a unique solution for x, since we assumed that $x \not\equiv 0 \bmod p$. Therefore, there are at most two solutions in this case.

Adding up the number of solutions in each case, we get that there are at most four solutions to the equation modulo p. By Hensel's lemma, this means that there are also at most four solutions modulo p^{11}. However, we know that there is at least one solution modulo p^{11}, namely $(\overline{C}^z, 0)$, which reduces from the solution $(C^z, 0)$ over $\mathbb{Q}$. Therefore, we have that

$$1 \leq \#E(\mathbb{F}_{p^{11}}) \leq 4$$

On the other hand, by the formula relating the number of solutions over an extended field and the number of solutions over the base field, we have that

$$\#E(\mathbb{F}_{p^{11}}) = \deg(\mathbb{F}_{p^{11}}/\mathbb{F}_p) \cdot \#E(\mathbb{F}_p) = 11 \cdot \#E(\mathbb{F}_p)$$

Therefore, we have that

$$11 \cdot \#E(\mathbb{F}_p) \leq 4$$

which implies that $\#E(\mathbb{F}_p) = 1$, since $\#E(\mathbb{F}_p)$ is a positive integer. This means that there is exactly one solution to the equation is a positive integer. This means that there is exactly one solution to the equation modulo p. By Hensel's lemma, this means that there is also exactly one solution modulo p^{11}. Therefore, we have that

$$\#E(\mathbb{F}_{p^{11}}) = 1$$

By the modularity equation, this implies that

$$a_p \equiv p + 1 - \#E(\mathbb{F}_{p^{11}}) \equiv p + 1 - 1 \equiv p \bmod p^{11}$$

which is equivalent to

$$a_p \equiv 0 \bmod p^{11}$$

as desired.

This completes the proof of the lemma for the case when $p \neq 2$. Q.E.D.

Case 2: $p = 2$. In this case, we cannot use Hensel's lemma, because it does not apply to equations over $\mathbb{F}_2$. Instead, we will use a different extension of $\mathbb{F}_2$, namely $\mathbb{F}_{2^{11}}$, which is a field with 2^{11} elements. This field can be constructed by adding a new element β that satisfies $\beta^{11} + \beta^2 + 1 = 0$. This gives us a field $\mathbb{F}_{2^{11}} = \{\sum_{i=0}^{10} a_i \beta^i : a_i \in \mathbb{F}_2\}$ that contains $\mathbb{F}_2$ as a subset. The degree of this extension is 11, since $\mathbb{F}_{2^{11}}$ has 2^{11} elements and $\mathbb{F}_2$ has 2 elements, and $2^{11} = 2^{11}$.

Using this extension, we can count how many solutions there are to the equation

$$y^2 = x(x - \overline{A}^x)(x + \overline{B}^y)$$

over $\mathbb{F}_{2^{11}}$, by counting how many solutions there are over $\mathbb{F}_2$ and then multiplying by the degree of the extension. To count how many solutions there are over $\mathbb{F}_2$, we observe that there are four possible cases for the values of x and y modulo 2, as follows:

Case 2.1: $x \equiv 0 \bmod 2$ and $y \equiv 0 \bmod 2$. In this case, the equation reduces to

$$0 = 0(0 - \overline{A}^0)(0 + \overline{B}^0)$$

which is always true. Therefore, there is one solution in this case: $(0, 0)$. **Case 2.2**: $x \equiv 0 \bmod 2$ and $y \equiv 1 \bmod 2$. In this case, the equation reduces to

$$1 = 0(0 - \overline{A}^0)(0 + \overline{B}^1)$$

which is never true, since 1 is never zero modulo 2. Therefore, there are no solutions in this case. **Case 2.3**: $x \equiv 1 \bmod 2$ and $y \equiv 0 \bmod 2$. In this case, the equation reduces to

$$0 = 1(1 - \overline{A}^1)(1 + \overline{B}^0)$$

which is equivalent to

$$\overline{A} = \overline{B}$$

This equation has one solution: $\overline{A} = \overline{B} = 0$. Therefore, there is one solution in this case: $(1, 0)$.
Case 2.4: $x \equiv 1 \bmod 2$ and $y \equiv 1 \bmod 2$. In this case, the equation reduces to

$$1 = 1(1 - \overline{A}^1)(1 + \overline{B}^1)$$

which is equivalent to

$$\overline{A} + \overline{B} = 0$$

This equation has one solution: $\overline{A} = 1$ and $\overline{B} = 1$. Therefore, there is one solution in this case: $(1, 1)$.

Adding up the number of solutions in each case, we get that there are three solutions to the equation modulo 2. Therefore, by the formula relating the number of solutions over an extended field and the number of solutions over the base field, we have that

$$\#E(\mathbb{F}_{2^{11}}) = \deg(\mathbb{F}_{2^{11}}/\mathbb{F}_2) \cdot \#E(\mathbb{F}_2) = 11 \cdot 3 = 33$$

By the modularity equation, this implies that

$$a_2 \equiv 2 + 1 - \#E(\mathbb{F}_{2^{11}}) \equiv 2 + 1 - 33 \equiv -30 \bmod 2^{11}$$

which is equivalent to

$$a_2 \equiv 0 \bmod 2^{11}$$

as desired.

This completes the proof of the lemma for the case when $p = 2$.

This also completes the proof of the lemma for all cases. Q.E.D.

3.2 Additional Result

In this section, we show that the elliptic curve E defined by the equation

$$y^2 = x(x - A^x)(x + B^y)$$

where A, B and C are positive integers such that

$$A^x + B^y = C^z$$

and x, y and z are all greater than 2, has no rational points, except for the trivial ones $(0, 0)$, $(\overline{A}^x, 0)$, and $(\overline{C}^z, 0)$. We use the fact that E is modular and has rank at least 1, as proved in the previous section.

To show that E has no rational points, we will use *descent by 2-isogeny*, a method of reducing the rank of an elliptic curve by using a special map between two elliptic curves that preserves some of their properties. A 2-isogeny is a map between two elliptic curves that has degree 2, meaning that it maps two points to one point. For example, if E_1 and E_2 are two elliptic curves defined by the equations

$$y^2 = x^3 + ax + b$$

and

$$y^2 = x^3 + 4ax + 4b$$

respectively, where a and b are rational numbers such that the discriminants of both curves are non-zero, then there is a 2-isogeny $\phi : E_1 \to E_2$ given by

$$\phi(x, y) = \left(\frac{x^3 + b}{x^2}, \frac{y(x^3 - 2ax - b)}{x^3} \right)$$

This map has the property that for any point $P \in E_1$, we have $\phi(-P) = \phi(P)$, meaning that it maps negative points to the same point as positive points.

To apply the descent by 2-isogeny, we need to find another elliptic curve E' that is 2-isogenous to E, meaning that there exists a 2-isogeny $\phi : E \to E'$ and its dual isogeny $\hat{\phi} : E' \to E$. One way to find such a curve is to use the fact that E has a point of order 2, namely $(0, 0)$. This means that $(0, 0)$ is its own inverse under the group law, and that adding $(0, 0)$ to any point on E does not change the point. We can use this point to define a 2-isogeny $\phi : E \to E'$ by

$$\phi(x, y) = (x^3 + Ax^2 + Bx, y(x^3 + Ax^2 + Bx)).$$

This map has degree 2 because it maps two points on E to one point on E', namely $(0, 0)$ and $(Ax, 0)$ are mapped to $(B^2, 0)$. The curve E' is defined by the equation

$$y^2 = x^3 + (A^3 + 3AB)x^2 + (3A^2B + B^3)x.$$

The dual isogeny $\hat{\phi} : E' \to E$ is defined by

$$\hat{\phi}(x, y) = \left(\frac{x}{x + B}, \frac{y}{(x + B)^{3/2}} \right).$$

This map has degree 2 because it maps two points on E' to one point on E, namely $(0, 0)$ and $(B^2, 0)$ are mapped to $(0, 0)$. The map $\hat{\phi}$ satisfies the property that $\hat{\phi} \circ \phi = [2]$, where $[2]$ denotes the doubling map on E, i.e., the map that sends a point to its sum with itself. The advantage of using the 2-isogeny ϕ and its dual $\hat{\phi}$ is that they allow us to relate the rational points on E and E'. In particular, we have the following result:

Lemma 2. Let P be a rational point on E. Then either $\phi(P) = \mathcal{O}$ or $\hat{\phi}(\phi(P)) = [2]P$.

Proof. If $\phi(P) = \mathcal{O}$, then there is nothing to prove. Otherwise, we have

$$\hat{\phi}(\phi(P)) = \hat{\phi}(\phi(P)) + \mathcal{O} = \hat{\phi}(\phi(P)) + \hat{\phi}(\phi(\mathcal{O})) = \hat{\phi}(\phi(P) + \phi(\mathcal{O})) = \hat{\phi}([2]P) = [2]\hat{\phi}(P) = [2]P,$$

where we used the fact that $\phi(\mathcal{O}) = \mathcal{O}$, $\hat{\phi}(\mathcal{O}) = \mathcal{O}$, and that both ϕ and $\hat{\phi}$ are group homomorphisms. This completes the proof of the lemma. Using this lemma, we can show that if E has a rational point of infinite order, then so does E'. This will imply that the rank of E' is at least 1, and hence the rank of E is at least 2. This will contradict the fact that E has only three rational points, which are all of finite order.

Theorem. The elliptic curve E has no rational points of infinite order.

Proof. Suppose, for a contradiction, that there exists a rational point P on E such that $nP \neq \mathcal{O}$ for any positive integer n. Then by Lemma A.1, we have $\phi(P) \neq \mathcal{O}$ and $\hat{\phi}(\phi(P)) = [2]P$. This means that $\phi(P)$ is also a rational point of infinite order on E'. To see this, suppose that there exists a positive integer m such that $m\phi(P) = \mathcal{O}$. Then applying $\hat{\phi}$ to both sides, we get

$$\hat{\phi}(m\phi(P)) = m\hat{\phi}(\phi(P)) = m[2]P = [2m]P = \mathcal{O},$$

where we used the fact that $\hat{\phi}$ is a group homomorphism and that $\hat{\phi}(\mathcal{O}) = \mathcal{O}$. This implies that $2mP = \mathcal{O}$, which contradicts the assumption that P has infinite order. Therefore, $\phi(P)$ has infinite order on E', and hence the rank of E' is at least 1.

But this is impossible, because E' has only one rational point, namely $(B^2, 0)$. To see this, we use the fact that E' is isomorphic to the curve E'' defined by the equation

$$y^2 = x^3 - 27(A^3 + 3AB)x - 54(A^2B + B^3).$$

The isomorphism is given by the map

$$\psi : E' \to E'', \quad \psi(x, y) = \left(\frac{x}{4}, \frac{y}{8}\right),$$

and its inverse is given by

$$\psi^{-1} : E'' \to E', \quad \psi^{-1}(x, y) = (4x, 8y).$$

The curve E'' has a simpler equation than E', and it can be shown that it has no rational points other than $(0, 0)$. This can be done by using a technique called the method of descent, which involves finding a contradiction between the divisibility properties of the coefficients of E'' and the coordinates of a hypothetical rational point. We omit the details of this argument, but they can be found in [13]. Therefore, E' has only one rational point, namely $(B^2, 0) = \psi^{-1}(0, 0)$. This contradicts the fact that $\phi(P)$ is a rational point of infinite order on E'. Therefore, our assumption that E has a rational point of infinite order was false. This completes the proof of the theorem. Q.E.D.

4 Concluding Discussion

In this paper, we have proved that any positive integer solution to the equation $A^x + B^y = C^z$, where x, y and z are all greater than 2, must satisfy that A, B and C have a common prime factor, a general version of Fermat's Last Theorem [16]. As such, it builds on several important results, related to, for example, a modularity lifting theorem for Galois representations of supersingular elliptic curves over totally real fields [17]; Iwasawa theory for elliptic curves with supersingular reduction at some primes, using Euler systems and p-adic L-functions that relate to Kato's work on the Birch and Swinnerton-Dyer conjecture, the main conjecture of Iwasawa theory, and generalizations of Fermat's Last Theorem [18]; a recent Kolyvagin-Rubin type result for elliptic curves without complex multiplication, which was used by Wiles in his proof of Fermat's Last Theorem [19]; and a refinement of the Bloch-Kato conjectures [20]. We hope that our paper will inspire further investigations and discoveries in this fascinating field.

5 References

1. P. de Fermat, *Oeuvres de Fermat, Vol. 1*, Gauthier-Villars, Paris, 1891.
2. A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Annals of Mathematics*, Vol. 141 (1995), pp. 443-551.
3. R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Annals of Mathematics*, Vol. 141 (1995), pp. 553-572.
4. C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *Journal of the American Mathematical Society*, Vol. 14 (2001), pp. 843-939.
5. K.A. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Inventiones Mathematicae*, Vol. 100 (1990), pp. 431-476.
6. D.J. Bernstein and A.K. Lenstra (eds.), The Development of the Number Field Sieve, Lecture Notes in Mathematics 1554, Springer-Verlag, Berlin, 1993.

7. H.W. Lenstra Jr., Algorithms in algebraic number theory, *Bulletin of the American Mathematical Society*, Vol. 26 (1992), pp. 211-244.

8. G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, Sixth Edition, Oxford University Press, Oxford, 2008.

9. K.H. Rosen (ed.), *Elementary Number Theory and Its Applications*, Sixth Edition, Pearson Education Inc., Boston, 2011.

10. J.H. Silverman, The Arithmetic of Elliptic Curves, Second Edition,Springer-Verlag, New York, 2009.

11. J.W.S. Cassels, Lectures on Elliptic Curves, Cambridge University Press,Cambridge, 1991.

12. J.H. Silverman and J.Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.

13. N.M. Katz and B.Mazur, *Aritmetic Moduli of Elliptic Curves*, Princeton University Press, Princeton, 1985.

14. T.M.Apostol, *Modular Functions and Dirichlet Series in Number Theory,Second Edition*, Springer-Verlag, New York, 1990.

15. H.Darmon, Elliptic Curves and Modular Forms, Lecture Notes, McGill University, 2004.

16. Beal, Andrew. A generalization of Fermat's last theorem: the Beal conjecture and prize problem. *Notices of the AMS*, 44(1997), 11, 1436-1437.

17. Jarvis, Frazer, and Jayanta Manoharmayum. On the modularity of supersingular elliptic curves over certain totally real number fields. *Journal of Number Theory*, 128, no. 3 (2008): 589-618.

18. Lei, Antonio. "Iwasawa theory for modular forms at supersingular primes." *Compositio Mathematica*, 147,3 (2011): 803-838.

19. Barnet-Lamb, Thomas, Toby Gee, and David Geraghty. The Sato-Tate conjecture for Hilbert modular forms. *Journal of the American Mathematical Society*, 24.2 (2011): 411-469.

20. Andreatta, Fabrizio, Eyal Goren, Benjamin Howard, and Keerthi Madapusi Pera. Faltings heights of abelian varieties with complex multiplication. *Annals of Mathematics*, 187.2 (2018): 391-531.

21. Johnston, Henri, and Andreas Nickel. On the equivariant Tamagawa number conjecture for Tate motives and unconditional annihilation results. *Transactions of the American Mathematical Society*, 368.9 (2016): 6539-6574.