ON THE GENERALIZED FERMAT EQUATION $a^2 + 3b^6 = c^p$

ANGELOS KOUTSIANAS

Abstract. In this paper, we prove that the equation $a^2 + 3b^6 = c^p$ has no non–trivial primitive integer solutions for $p \geq 239$. Our proof is based on the modularity of Galois representations of $\mathbb{Q}$–curves and the work of Ellenberg [Ell04].

1. Introduction

The remarkable breakthrough of Andrew Wiles about the proof of Taniyama–Shimura conjecture which leaded to the proof of Fermat’s Last Theorem introduced a new and very rich area of modern number theory. A variety of techniques and ideas have been developed for solving the generalized Fermat equation of the form

$$Aa^p + Bb^q = Cc^r.$$ 

Because the literature is very rich we refer to [BCDY15] for a detailed exposition of the cases of (1) that have been solved. In this paper we prove the following

Theorem 1. Let $p \geq 239$ be an odd prime. The equation

$$a^2 + 3b^6 = c^p$$

does not have non–trivial primitive solutions. A solution $(a, b, c)$ is called primitive if $a, b, c$ are pairwise coprime integers and non–trivial if $ab \neq 0$.

The paper is organised as follows. In Section 2 we recall the terminology and theory of $\mathbb{Q}$–curves. In Section 3 we introduce a Frey curve which we prove it is a $\mathbb{Q}$–curve and we study its arithmetic properties. In Section 4 we prove Theorem 1 while in Section 5 we explain and apply Ellenberg’s analytic method [Ell04]. Finally, in Section 6 we compute an explicit upper bound of $|E(\mathbb{Q})|$ in Theorem 2.

The computations of the paper were performed in Magma [BCP97] and the programs can be found in author’s homepage [https://sites.google.com/site/angeloskoutsianas/]

2. Preliminaries

In the section we recall the main definitions of the $\mathbb{Q}$–curves and their attached representations; we recommend [BC12, ES01, Que00] and [Rib04] for a more detailed exposition.

Let $K$ be a number field and $E/K$ be an elliptic curve without CM such that for every $\sigma \in G_K$ there exists an isogeny $\mu_E(\sigma) : E \to E$. Then $E$ is called a $\mathbb{Q}$–curve defined over $K$. We make a choice of the isogenies above such that $\mu_E$ is locally constant.

Date: June 1, 2018.

2010 Mathematics Subject Classification. Primary 11D61.

Key words and phrases. Fermat equations, $\mathbb{Q}$–curves, Galois representations.
Let
\[ c_E(\sigma, \tau) = \mu_E(\sigma)^\sigma \mu(\tau) \mu(\sigma \tau)^{-1}, \in (\text{Hom}(E, E) \otimes \mathbb{Q})^* = \mathbb{Q}^* \]
where \( \mu_E^{-1} := (1/\deg \mu_E) \mu_E^* \) and \( \mu_E^* \) is the dual of \( \mu_E \). Thus \( c_E \) determines a class in \( H^2(G_\mathbb{Q}, \mathbb{Q}^*) \) which depends only on the \( \mathbb{Q} \)-isogeny class of \( E \). Tate has showed that \( H^2(G_\mathbb{Q}, \mathbb{Q}^*) \) is trivial when \( G_\mathbb{Q} \) acts trivially on \( \mathbb{Q}^* \). So, there exists a continuous map \( \beta : G_\mathbb{Q} \to \mathbb{Q}^* \) such that
\[ c_E(\sigma, \tau) = \beta(\sigma) \beta(\tau) \beta(\sigma \tau)^{-1} \]
The map \( \beta \) is called a splitting map of \( c_E \).

We define an action of \( G_\mathbb{Q} \) on \( E_p \otimes \mathbb{Q}_p \) given by
\[ \hat{\rho}_{E,p}(\sigma)(1 \otimes x) = \beta(\sigma)^{-1} \otimes \mu(\sigma)(\sigma(x)) \]
From the definition of \( \hat{\rho}_{E,p} \) we have that \( \mathbb{P} \hat{\rho}_{E,p} |_{G_K} \cong \mathbb{P} \hat{\rho}_{E,p} \) where
\[ \hat{\rho}_{E,p} : \text{Gal}(\bar{K}/K) \to \text{GL}_2(\mathbb{Z}_p) \]
is the usual Galois representation attached to the \( p \)-adic Tate module of \( E \) (see [ES01, Proposition 2.3]). Given a splitting map \( \beta \), Ribets [RI91] attaches an abelian variety \( A_\beta \) over \( \mathbb{Q} \) of \( \text{GL}_2 \)-type such that \( E \) is a simple factor over \( \mathbb{Q} \).

From the definition of \( \hat{\rho}_{E,p} \) we understand that the representation depends on \( \beta \). Let \( M_\beta \) be the field generated by the values of \( \beta \). We want to make a choice of \( \beta \) such that it factors over a number field of low degree and \( c_E(\sigma, \tau) = \beta(\sigma) \beta(\tau) \beta(\sigma \tau)^{-1} \) as elements in \( H^2(G_\mathbb{Q}, \mathbb{Q}^*) \). Then we choose a twist \( E_\beta/K_\beta \) such that \( c_{E_\beta}(\sigma, \tau) = \beta(\sigma) \beta(\tau) \beta(\sigma \tau)^{-1} \) as cocycles and \( K_\beta \) is the splitting field of \( \beta \). In this case, the abelian variety \( A_\beta \) is a quotient of \( \text{Res}_{K_\beta/Q} E_\beta \) over \( \mathbb{Q} \). The endomorphism algebra of \( A_\beta \) is equal to \( M_\beta \) and the representation on the \( \pi_n \)-torsion points of \( A_\beta \) coincides with the representation \( \hat{\rho}_{E,p} \) above, where \( \pi \) is a prime ideal in \( M_\beta \) above \( p \).

Finally, we define the \( \epsilon : G_\mathbb{Q} \to \mathbb{Q}^* \) given by
\[ \epsilon(\sigma) = \frac{\beta(\sigma)^2}{\deg \mu(\sigma)} \]
Then, \( \epsilon \) is a character such that
\[ \det(\hat{\rho}_{E,p}) = \epsilon^{-1} \cdot \chi_p \]
where \( \chi_p \) is the the \( p \)-th cyclotomic character. We can attach a residual representation associate to \( \hat{\rho}_{E,p} \) (see [ES01, p. 107])
\[ \rho_{E,p} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_p^* \text{GL}_2(\mathbb{F}_p). \]
Similarly, we denote by \( \phi_{E,p} \) the residual representation associate to \( \hat{\phi}_{E,p} \).

3. Frey \( \mathbb{Q} \)-curve attached to \( a^2 + 3b^6 = c^3 \)

In this section we attach a Frey \( \mathbb{Q} \)-curve over \( K = \mathbb{Q}(\sqrt{3}) \) to a primitive solution \((a, b, c)\) of \([2]\). Let \( p \) be an odd prime. We define
\[ E : Y^2 = X^3 - 9\sqrt{-3}b(4a - 5\sqrt{-3}b^3)X + 18(2a^2 - 14\sqrt{-3}ab^3 - 33b^6) \]
The invariants of $E$ are given by

\begin{align}
(11) \quad j(E) &= 432 \cdot \sqrt{-3} \cdot b^3 \cdot \frac{(4a - 5\sqrt{-3}b^3)^3}{(a + \sqrt{-3}b^3)^3 \cdot (a - \sqrt{-3}b^3)^3}, \\
(12) \quad \Delta(E) &= -2^8 \cdot 3^7 \cdot (a - \sqrt{-3}b^3) \cdot (a + \sqrt{-3}b^3)^3, \\
(13) \quad c_4(E) &= 2^4 \cdot 3^3 \cdot \sqrt{-3} \cdot b \cdot (4a - 5\sqrt{-3}b^3), \\
(14) \quad c_6(E) &= -2^6 \cdot 3^5 \cdot (2a^2 - 14\sqrt{-3}b^3a - 33b^6).
\end{align}

**Lemma 3.1.** Let $a/b^3 \in \mathbb{P}^1(\mathbb{Q})$. Then the $j$–invariant of $E$ lies in $\mathbb{Q}$ only when

- $a/b^3 = 0$ and $j = 54000$, or
- $a/b^3 = \infty$ and $j = 0$.

**Proof.** From (11) and for $a/b^3 = \infty$ we have that $j = 0$. Let assume that $a/b^3 \neq \infty$. After cleaning denominators of (11) and taking real and imaginary parts using the restriction that $j,a/b \in \mathbb{Q}$ we end up with

\begin{align}
\begin{align*}
-A^4 j' + 720A^2 + 9j' - 1125 &= 0 \\
(-A^2 j' + 32A^2 - 3j' - 450)A &= 0,
\end{align*}
\end{align}

where $j' = j/432$ and $A = a/b^3$. From the second equation we have that either $A = 0$ or $j' = \frac{32A^4 - 450}{A^2 + 3}$. For $A = 0$ we have the first case of the lemma. Replacing $j'$ to the first equation above we end up with

\begin{align}
(15) \quad -32A^4 + 1266A^2 - 2475 &= 0.
\end{align}

which we can easily check that does not have any solution over $\mathbb{Q}$. 

**Lemma 3.2.** The curve $E$ does not have complex multiplication unless

- $a/b^3 = 0$, $j = 54000$ and $d(O) = -12$ or
- $a/b^3 = \infty$, $j = 0$ and $d(O) = -3$.

**Proof.** Let assume that $E$ has complex multiplication. Then from the theory of complex multiplication we know that the $j(E)$ is a real algebraic number. Because $j(E) \in \mathbb{Q}(\sqrt{-3})$ we conclude that $j(E) \in \mathbb{Q}$. Because the list of $j$–invariants of elliptic curves with complex multiplication with $j \in \mathbb{Q}$ it is known (see [Cox89]) we have the result.

**Lemma 3.3.** Let $(a,b,c)$ be a non–trivial primitive solution of (2), then $c$ is divisible by a prime different from 2 and 3.

**Proof.** Because $(a,b,c)$ is a solution of $a^2 + 3b^6 = c^p$ we have that $3 \mid c$. Because $p \geq 3$ and $a^2 + 3b^6 \neq 0 \mod 8$ we have that $2 \not\mid c$. 

Because of Lemma [km2] we assume that $E$ has no complex multiplication. The curve $E$ is a $\mathbb{Q}$–curve because it is 3–isogenous to its conjugate and the isogeny is defined over $K$ (see IsQcurve.m). We make a choice of isogenies $\mu(\sigma) : E \rightarrow E$ such that $\mu(\sigma) = 1$ for $\sigma \in G_K$ and $\mu(\sigma)$ equal to the 3–isogeny above for $\sigma \not\in G_K$.

Let $d$ be the degree map (see [Que00]), then we have that $d(G_3) = \{1,3\} \subset \mathbb{Q}^*/\mathbb{Q}^{*2}$. The fixed field $K_d$ of the kernel of the degree map is $\mathbb{Q}(\sqrt{-3})$. Then $(a,d) = (-3,3)$ is a dual basis in the terminology of [Que00]. We can see that $(-3,3)$ is unramified and so $c = 1$, $K_c = \mathbb{Q}$ and $K_\beta = \mathbb{Q}(\sqrt{-3})$. Moreover, we have $\beta(\sigma) = \sqrt{d(\sigma)}$ and so $M_\beta = \mathbb{Q}(\sqrt{3})$. 
Let \( A_\beta = \text{Res}_{K/Q} E \). Since \( K_\beta = K \) we understand that \( \xi_K(E) \) has trivial Schur class. Thus from \cite{Que00} Theorem 5.4 we have that \( A_\beta \) is a \( GL_2 \)-type variety with \( \mathbb{Q} \)-endomorphism algebra isomorphic to \( M_\beta \).

Let \( p_2 \) and \( p_3 \) be the primes in \( K \) above 2 and 3 respectively.

**Lemma 3.4.** The elliptic curve \( E \) is a minimal model with conductor equal to \( \left[ 2 \right] \). Let \( A_\beta = E \). Since \( K_\beta = K \) we understand that \( \xi_K(E) \) has trivial Schur class. Thus from \cite{Que00, Theorem 5.4} we have that \( A_\beta \) is a \( GL_2 \)-type variety with \( \mathbb{Q} \)-endomorphism algebra isomorphic to \( M_\beta \).

Let \( p_2 \) and \( p_3 \) be the primes in \( K \) above 2 and 3 respectively.

**Lemma 3.5.** The conductor of \( A_\beta \) is
\[
\left( \frac{d_{K_\beta/Q} \cdot \text{Norm}_{K_\beta/Q}(N(E))}{2^4 \cdot 3^{10} \cdot \prod p^2} \right). 
\]

**Proposition 3.6.** The representation \( \phi_{E,p} \mid_{I_p} \) is finite flat for \( p \neq 2, 3 \).

**Proof.** Let \( p \) be a prime above \( p \). ByLemma 3.4 we know that \( E \) has good or multiplicative reduction at \( p \). In the case of multiplicative reduction the exponent of \( p \) in the minimal discriminant of \( E \) is divisible by \( p \). Finally, \( K \) is only ramified at 3 and so \( I_p \subseteq G_K \).

**Proposition 3.7.** The representation \( \phi_{E,p} \mid_{I_\ell} \) is trivial for \( \ell \neq 2, 3, p \).

\footnote{For some of the computations it is more convenient to use the isomorphic to \( E \) curve \( E' : Y^2 + 6\sqrt{-3}bXY - 12(\sqrt{-3}b^3 + a)Y = X^3 \).}
ON THE GENERALIZED FERMAT EQUATION $a^2 + 3b^6 = c^p$

Proof. Let $l$ be a prime above $ℓ$. Because of Lemma 3.4 we know that $E$ has good or multiplicative reduction at $l$. In the case of multiplicative reduction the exponent of $l$ in the minimal discriminant of $E$ is divisible by $p$. Finally, $K$ is only ramified at 3 and so $I_ℓ ⊆ G_K$. □

Proposition 3.8. Suppose $p \neq 2, 3$. Then $N_ρ = 972$.

Proof. Because we want to compute the Artin conductor of $ρ_{E,p}$, we consider only ramification at primes above $ℓ \neq 2, 3$. Let consider $ℓ \neq 2, 3, p$. We recall that $K = K_β$. Because $ℓ \neq 3$ we have that $K_β$ is unramified at $ℓ$, so $I_ℓ ⊆ G_K$. Because $ρ_{E,p}|G_K \simeq φ_{E,p}$ and $φ_{E,p} | I_ℓ$ is trivial we have that $ρ_{E,p}$ is trivial at $I_ℓ$. Thus, $ρ_{E,p}$ is unramified outside $2, 3, p$.

Suppose $ℓ = 2, 3$. From (11) we understand that $E$ has potential good reduction at primes above $2, 3$. That means that $φ_{E,p}|I_ℓ$ factors through a finite group of order divisible only by $2, 3$. Thus, $ρ_{E,p}|I_ℓ$ factors through a finite group of order divisible only by $2, 3$. It follows that the exponent of $ℓ$ in the conductor of $ρ_{E,p}$ is the same as in the conductor of $ρ_{E,p}$ as $p \neq 2, 3$. □

Proposition 3.9. Suppose $p \neq 2, 3$. Then $k_ρ = 2$.

Proof. The weight is determined by $ρ_{E,p}|I_p$. For $p \neq 3$ we have that $K$ is unramified at $p$ and so $I_p ⊆ G_K$. Because $ρ_{E,p}|G_K \simeq φ_{E,p}$, $φ_{E,p} | I_p$ is finite flat and the determinant of $φ_{E,p}$ is the cyclotomic $p$–th character then from [Ser87, Prop. 4] we have the conclusion. □

Proposition 3.10. The character $ε_ρ$ is trivial.

Proof. This is a consequence of the fact that $ε$ is trivial and the properties of $ρ_{E,p}$. □

From [EH04 Proposition 3.2] and Lemma 3.3 we have

Proposition 3.11. Let assume that $ρ_{E,p}$ is reducible for $p \neq 2, 3, 5, 7, 13$. Then $E$ has potentially good reduction at all primes above $ℓ > 3$.

4. PROOF OF THEOREM

Proof. Let assume that $p \geq 239$ be an odd prime. Let $(a, b, c)$ be a non–trivial primitive solution of (2). We attach to $(a, b, c)$ the curve $E$. Because of the modularity of $Q$–curves which follows from Serre’s conjecture (see [KW99a], [KW99b], [Kis09]), the Ribet’s level lowering [Rib90] and the results in Section 3 we have that there exists a newform $f ∈ S_2(Γ_0(972))$ such that $ρ_{E,p} \simeq ρ_{f,p}$.

There are 7 newforms of level 972. Four of them are rational with complex multiplication by $Q(√−3)$ and the other three are irrational. In Section 5 we show how we can prove that non–solutions arise from the rational newforms, see Proposition 5.6. For the irrational newforms we use Proposition 4.1 and we prove that $p ≤ 7$ (see CongruenceCriterion.m). □

2Let $f$ be a newform and $K_f$ the eigenvalues field of $f$. Then we say that $f$ is rational when $K_f = Q$ and irrational when $K_f \neq Q$. 
Proposition 5.1. Let \( f \in S_2(\Gamma_0(972)) \) and \( p, q \) be primes such that \( p \geq 11 \), \( q \geq 5 \) and \( q \neq p \). We define

\[
B(q, f) = \begin{cases} 
N(a_q(E) - a_q(f)) & \text{if } a^2 + 3b^6 \equiv 0 \mod q \text{ and } \left( \frac{a^2}{q} \right) = 1, \\
N(a_q(f)^2 - a_q(E) - 2q) & \text{if } a^2 + 3b^6 \equiv 0 \mod q \text{ and } \left( \frac{a^2}{q} \right) = -1, \\
N((q + 1)^2 - a_q(f)^2) & \text{if } a^2 + 3b^6 \equiv 0 \mod q.
\end{cases}
\]

where \( a_q(E) \) is the trace of \( \text{Frob}_q \) acting on the Tate module \( T_p(E) \). Then \( p | B(q, f) \).

Proof. From Section 3 we recall that \( A_{\beta} = \text{Res}_{K/Q}(E) \) and \( M_{\beta} = \mathbb{Q}(\sqrt{3}) \). Let \( \pi \) be a prime of \( M_{\beta} \) above \( p \). As we mentioned in Section 2 we have that \( \rho_{\beta, \pi} = \rho_{E, p} \) where \( \rho_{\beta, \pi} \) is the mod \( \pi \) representation of \( G_Q \) on the \( \pi^n \)-torsion points of \( A_{\beta} \). We recall that

\[
\rho_{E, p}(\sigma)(1 \otimes x) = \beta(\sigma)^{-1} \otimes \mu(\sigma)(\phi_{E, p}(\sigma)(x))
\]

where \( \phi_{E, p} \) is the representation of \( G_K \) acting on \( T_p(E) \) and \( 1 \otimes x \in M_{\beta, \pi} \otimes T_p(E) \). We also recall that \( \rho_{\beta, \pi} = \rho_{E, p} \simeq \rho_{f, p} \) and \( \beta(\sigma) = \sqrt{d(\sigma)} \).

Let assume the case \( a^2 + 3b^6 \equiv 0 \mod q \). By \([13]\) we have that \( q || N_{A_{\beta}} \) and from \([20]\) we have that \( p | N(a_q(f)^2 - (q + 1)^2) \).

For the rest of the proof we assume that \( a^2 + 3b^6 \equiv 0 \mod q \). When \( \left( \frac{a^2}{q} \right) = 1 \) we have that \( \sigma = \text{Frob}_q \in G_K \) and \( \mu(\sigma) = 1 \), \( d(\sigma) = 1 \), so \( \text{Tr} \rho_{\beta, \pi}(\sigma) = \text{Tr} \phi_{E, p}(\sigma) \).

Because \( \rho_{\beta, \pi} = \rho_{E, p} \simeq \rho_{f, p} \) we conclude that \( a_q(E) \equiv a_q(f) \mod \pi \) and so \( p | N(a_q(E) - a_q(f)) \).

Suppose \( \left( \frac{a^2}{q} \right) = -1 \), then \( \sigma = \text{Frob}_q \not\in G_K \). Because \( \sigma^2 \in G_K \) and similarly to the above lines we have that \( \text{Tr} \rho_{\beta, \pi}(\sigma^2) = \text{Tr} \phi_{E, p}(\sigma^2) = a_{q^2}(E) \). We know that

\[
\frac{1}{\det(I - \rho_{\beta, \pi}(\sigma)q^{-s})} = \exp \sum_{n=1}^{\infty} \frac{\text{Tr} \rho_{\beta, \pi}(\sigma^n) q^{-ns}}{n} = \frac{1}{1 - \text{Tr} \rho_{\beta, \pi}(\sigma)q^{-s} + q^{-2s}}
\]

From the coefficient of \( q^{-2s} \) we have that \( \text{Tr} \rho_{\beta, \pi}(\sigma^2) = \text{Tr} \rho_{E, p}(\sigma^2) = a_{q^2}(E) - 2q \). As above we conclude that \( a_q(f)^2 \equiv a_{q^2}(E) + 2q \mod \pi \), so \( p | N(a_q(f)^2 - a_{q^2}(E) - 2q) \). \( \square \)

5. Eliminating the CM forms

In this section we explain and apply the method of Ellenberg \([13]\) which allows us to prove that no solutions of \( \mathbb{F}_p \) arise from the rational newforms for \( p > 239 \).

Proposition 5.1 (Proposition 3.4 \([13]\)). Let \( K \) be an imaginary quadratic field and \( E/K \) a \( \mathbb{Q} \)-curve of squarefree degree \( d \). Suppose the image of \( \mathbb{F}_{p}E \) lies in the normalizer of a split Cartan subgroup of \( \text{PGL}_2(\mathbb{F}_p) \), for \( p = 11 \) or \( p > 13 \) with \( (p, d) = 1 \). Then \( E \) has potentially good reduction at all primes of \( K \) not dividing \( 6 \).

Proposition 5.2 (Proposition 3.6 \([13]\)). Let \( K \) be an imaginary quadratic field and \( E/K \) a \( \mathbb{Q} \)-curve of squarefree degree \( d \). Then there exists a constant \( M_{K, d} \) such that if the image of \( \mathbb{F}_{p}E \) lies in the normalizer of a nonsplit Cartan subgroup of \( \text{PGL}_2(\mathbb{F}_p) \) and \( p > M_{K, d} \) then \( E \) has potential good reduction at all primes of \( K \).
The constant $M_{K,d}$ can be chosen to be a lower bound of the primes Proposition \ref{prop3.2} holds.

**Proposition 5.3** (Proposition 3.9 \cite{Ell04}). Let $K$ be an imaginary quadratic field and $\chi_K$ be the associate Dirichlet character. Then for all but finitely many primes $p$, there exists a weight 2 cusp form $f$, which is either

- a newform in $S_2(\Gamma(dp^2))$ with $w_pf = f$ and $w_pf = -f$,
- a newform in $S_2(\Gamma(d'p^2))$ with $d'$ a proper divisor of $d$ and $w_pf = f$

such that $A_{f\otimes\chi}(\mathbb{Q})$ is a finite group.

The reasons why Proposition \ref{prop5.3} implies Proposition \ref{prop5.2} are explained in \cite{Ell04, Ell05}. From the practical point of view it is important to make the above estimates explicit.

Let $f$ be a modular form with $q$–expansion

$$f = \sum_{m=0}^{\infty} a_m(f)q^m. \quad (22)$$

We define $L_\chi(f) := L(f \otimes \chi, 1)$ where $\chi$ is a Dirichlet character. We can think $a_m$ and $L_\chi$ as linear functions in the space of modular forms.

Moreover, we denote by $\mathcal{F}$ a Petersson–orthonormal basis for $S_2(\Gamma_0(N))$ and define

$$\langle a_m, L_\chi \rangle_N := \sum_{f \in \mathcal{F}} a_m(f)L_\chi(f) \quad (23)$$

For $M \mid N$ we denote by $(a_m, L_\chi)_N^M$ the contribution to $(a_m, L_\chi)_N$ of the forms which are new at level $M$. We also define

$$(a_m, L_\chi)_{p^2}^{p-\text{new}} := (a_m, L_\chi)_{p^2} - (a_m, L_\chi)_{p^2}^0. \quad (24)$$

In \cite{Ell04} it is explained that Proposition \ref{prop5.3} holds as long as $|(a_1, L_\chi)_{p^2}^{p-\text{new}}| > 0$. For $p$ sufficiently large $|(a_1, L_\chi)_{p^2}^{p-\text{new}}| > 0$ because $(a_1, L_\chi)_{p^2} = 4\pi + O(p^{-2}\log^2 p)$ and $(a_1, L_\chi)_{p^2}^0 = O(p^{-1})$ \cite{Ell04, Ell05}. From the practical point of view it is important to make the above estimates explicit.

From \cite{Ell04} Lemma 3.12 we have

$$\langle a_m, L_\chi \rangle_{p^2} = \frac{p}{p^2 - 1}(a_m - p^{-1}\chi(p)a_{mp}, L_\chi)_p. \quad (25)$$

We use the following result in \cite{Ell04} to bound $(a_m, L_\chi)_p$ for $m = 1, p$.

**Lemma 5.4.** Let $p$ be a prime, $m$ a positive integer, $\chi$ a quadratic character of conductor $q$ prime to $p$. Then

$$|(a_m, L_\chi)_p| \leq 2\sqrt{3}m^{1/2}d(m)(1 - e^{-2\pi/q\sqrt{p}})^{-1}(4\pi + 16\xi^2(3/2)p^{-3/2}). \quad (26)$$

So, from Lemma \ref{lem5.4} and \ref{eq25} we have an explicit bound for $|(a_1, L_\chi)_{p^2}|$. We focus on $(a_m, L_\chi)_{p^2}$ now. In \cite{Ell05} the author proves the following

**Theorem 2** (\cite{Ell05}). Suppose $N \geq 400$, $N \nmid q$ where $q$ is the conductor of $\chi$ and let $\sigma$ be a real number with $q^2/2\pi \leq \sigma \leq Nq/\log N$. Then

$$\langle a_m, L_\chi \rangle_N = 4\pi \chi(m)e^{-2\pi m/\sigma N\log N} - E_3 - E_2 - E_1 + (a_m, B(\sigma N\log N)) \quad (27)$$

where

- $|(a_m, B(\sigma N\log N))| \leq 30(400/399)^3 2\pi q^2 m^{3/2} N^{-1/2}d(N)N^{-2\pi/q^2}$
\begin{itemize}
\item \(|E_1| \leq (16/3)\pi^3 m^{3/2} \sigma \log N e^{-N/2 \pi m \sigma \log N}\)
\item \(|E_2| \leq (3/8) \pi^3 \zeta(3/2) m^{5/2} \sigma^2 N^{-3/2} \log^2 N\)
\item \(|E_3| \leq (8/3) \zeta(3/2) \pi^3 \sigma m^{3/2} N^{-1/2} \log N d(N) e^{-N/2 \pi m \sigma \log N}\)
\item \(|E(3)| \leq 16 \pi^3 m \sum_{c > 0, N | c} \min \{ \frac{2}{\pi} \phi(q) c^{-1} \log c, \frac{1}{\sigma} \sigma N \log N m^{1/2} c^{-3/2} d(c) \} \).
\end{itemize}

The only upper bound that it is not explicit is the one for \(E(3)\). In Section 6 we give an explicit upper bound for the case \(m = 1\) in terms of \(q\) and \(N\).

In our case we have \(d = 3\), \(\chi_{-3} = (\frac{\cdot}{3})\) and \(q = 3\). We have written a Magma script which shows that \(|(a_1, L_\chi)^{p_{\text{new}}} > 0|\) for \(p \geq 239\) (see AnalyticMethod.m).

So we have proved the following.

**Proposition 5.5.** Let \(p \geq 239\) be a prime. Then there exists a newform \(f \in S_2(\Gamma_0(p^2))\) such that \(w_p f = f\) and \(L(f \otimes \chi_{-3}) \neq 0\).

**Remark:** For \(p < 239\) the method in Ellenberg’s method requires to compute newforms of the space \(S_2(\Gamma_0(p^2))\) which is computationally hard problem when \(p\) is large.

**Proposition 5.6.** Let \(p \geq 239\) be a prime. Then non–trivial primitive solutions of \((28)\) do not arise from a rational newform \(f \in S_2(\Gamma_0(972)).\)

**Proof.** Let \(f\) be a rational newform of \(S_2(\Gamma_0(972))\). Then we know that \(f\) has complex multiplication and so the image of \(\rho_{f,p}\) lies in the normalizer of a Cartan group. Because of Lemma 6.3 there exists a prime in \(K\) not above 6 such that \(E\) does not has potential good reduction. Because of Propositions 5.1, 5.2 and 5.3 we have that \(\rho_{E,p}\) does not lie in the normalizer of a Cartan group. However, this is a contradiction to the fact that \(\rho_{E,p} \simeq \rho_{f,p}\).

\[\square\]

6. Upper bound for \(|E(3)|\)

Here we give upper bounds for \(E(3)\) in [Ell05] for \(m = 1\). Then we have

**Proposition 6.1.** Let \(N \geq 400\) be the level of the newforms and \(q\) be the conductor of the character. Then we have

\[|E(3)| \leq 16 \pi^3 \left( \frac{2 \phi(q)}{\pi} \cdot \frac{3 \log N (2 \log N + 2)}{N} + \frac{\sqrt{3} \sigma \log N}{6} \cdot \frac{4 \log N + 4 \gamma + 4.4}{N} \right).\]

**Proof.** From [Ell05] we have that

\[|E(3)| \leq 16 \pi^3 \left( \frac{2 \phi(q)}{\pi} \sum_{0 < c < N^2} \frac{\log(cN)}{cN} + \frac{\sigma N \log N}{6} \sum_{c \geq N^2} \frac{d(cN)}{(cN)^{3/2}} \right)\]

Then from lemmas 6.2 and 6.3 we have the result. \(\square\)

**Lemma 6.2.** Let \(N\) be a positive integer, then

\[\sum_{c < N^2} \frac{\log(cN)}{cN} \leq \frac{3 \log N (2 \log N + 2)}{N}\]

\[\text{For the computations of the upper bound of } E(3) \text{ we choose } \sigma = q^2/2\pi.\]
ON THE GENERALIZED FERMAT EQUATION $a^2 + 3b^6 = c^p$

**Proof.** We have that

\[ \sum_{c < N^2} \frac{\log(cN)}{cN} = \frac{3 \log N}{N} \left( \sum_{c < N^2} \frac{1}{c} \right). \]

However, we can prove that (see [Apo76, Chapter 3])

\[ \sum_{c < N^2} \frac{1}{c} \leq 2 \log N + 2. \]

□

**Lemma 6.3.** For $N \geq 32$ we have

\[ \sum_{c \geq N^2} \frac{d(cN)}{(cN)^{3/2}} \leq \frac{\sqrt{3}}{N} \left( \frac{4 \log N + 4\gamma + 4.4}{N} \right) \]

where $\gamma$ is Euler’s constant.

**Proof.** We have that

\[ \sum_{c \geq N^2} \frac{d(cN)}{(cN)^{3/2}} \leq \frac{\sqrt{3}}{N} \sum_{c \geq N^2} \frac{d(c)}{c^{3/2}} \]

because $d(n) \leq \sqrt{3n}$ and $d(cN) \leq d(c)d(N)$. From [BEN10] Lemma 13] we have that

\[ \sum_{c \geq x} \frac{d(c)}{c^{3/2}} \leq \frac{2 \log x + 4\gamma + 4.4}{x^{1/2}} \]

for $x \geq 1000$ where $\gamma$ is Euler’s constant which completes the proof. □

**Acknowledgement**

The author would like to thank Professor John Cremona for providing access to the servers of the Number Theory Group of Warwick Mathematics Institute where all the computations took place.

**References**

[Apo76] Tom M. Apostol. *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics. Springer-Verlag New York, 1976.

[BC12] Michael A. Bennett and Imin Chen. Multi-Frey $\mathbb{Q}$-curves and the diophantine equation $a^2 + b^6 = c^n$. *Algebra Number Theory*, 6(4):707–730, 2012.

[BCDY15] Michael A. Bennett, Imin Chen, Sander R. Dahmen, and Soroosh Yazdani. Generalized Fermat equations: A miscellany. *Int. J. Number Theory*, 11(01):1–28, 2015.

[BEN97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BEN10] Michael A. Bennett, Jordan S. Ellenberg, and Nathan C. Ng. The diophantine equation $a^4 + b^6 = c^n$. *Int. J. Number Theory*, 6(02):311–338, 2010.

[Car86] H. Carayol. Sur les représentations $\ell$-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup.*, 19:409–468, 1986.

[Che10] I. Chen. On the equation $a^2 + b^6 = c^3$. *Acta Arith.*, 143:345–375, 2010.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, 1989.

[DDT97] H. Darmon, F. Diamond, and R. Taylor. *Elliptic curves, modular forms & Fermat’s Last Theorem* (Hong Kong, 1993), chapter Fermat’s Last Theorem, pages 2–140. International Press, 1997.
[Ell04] Jordan Ellenberg. Galois representations attached to \mathbb{Q}-curves and the generalized Fermat equation $a^4 + b^2 = c^p$. *American Journal of Mathematics*, 126(4):763–787, 2004.

[Ell05] Jordan Ellenberg. On the Error Term in Dukes Estimate for the Average Special Value of $l$-Functions. *Canad. Math. Bull.*, 48(4):535–546, 2005.

[ES01] Jordan S. Ellenberg and Chris Skinner. On the modularity of \mathbb{Q}-curves. *Duke Math. J.*, 109(1):97–122, 07 2001.

[Kis09] Mark Kisin. Modularity of 2-adic Barsotti–Tate representations. *Invent. Math.*, 178(3):587–634, 2009.

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre’s modularity conjecture (I). *Invent. Math.*, 178(3):485–504, 2009.

[KW09b] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre’s modularity conjecture (II). *Invent. Math.*, 178(3):505–586, 2009.

[Mil72] J. S. Milne. On the arithmetic of abelian varieties. *Invent. Math.*, 17(3):177–190, 1972.

[Pap93] I. Papadopoulos. Neron classification of elliptic curves where the residual characteristics equal 2 or 3. *Journal of Number Theory*, 44(2):119 – 152, 1993.

[Que00] Jordi Quer. \mathbb{Q}-curves and abelian varieties of GL$_2$-type. *Proc. London Math. Soc.*, 81(2):285–317, 2000.

[Rib90] K. A. Ribet. On modular representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *Invent. Math.*, 100(1):431–476, 1990.

[Rib04] Kenneth A. Ribet. *Abelian Varieties over \mathbb{Q} and Modular Forms*, pages 241–261. Birkhäuser Basel, Basel, 2004.

[Ser87] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.