BULLETIN OF THE
HELLENIC MATHEMATICAL SOCIETY
Volume 64, 2020 (56–68)

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

ANGELOS KOUTSIANAS

Abstract. We prove that the only primitive solutions of the equation

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

for $n \geq 3$ are $(a, b, c, n) = (\pm 47, \pm 2, \pm 7, 4)$. Our proof is based on the modularity of Galois representations of $\mathbb{Q}$-curves and the work of Ellenberg [Ell04] for big values of n and a variety of techniques for small n.

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

$$Aa^p + Bb^q = Cc^r. \tag{1}$$

Because the literature is very rich we refer to [BCDY15] for a detailed exposition of the cases of (1) that have been solved. A solution of (1) is called *primitive* if a, b, c are pairwise coprime integers and $abc \neq 0$.

In this paper we prove the following.

Theorem 1. *Let $n \geq 3$ be an integer. The only primitive solutions of equation*

$$a^2 + 3b^6 = c^n, \tag{2}$$

are $(a, b, c, n) = (\pm 47, \pm 2, \pm 7, 4)$.

For the proof of Theorem 1 we use the recent proof of modularity of $\mathbb{Q}$-curves as a consequence of Serre's modularity conjecture [KW09a, KW09b, Kis09] and the study of the arithmetic of $\mathbb{Q}$-curves by many mathematicians [Que00, Ell04, Rib04]. Even though we are not able to give a detailed proof, it seems that for the equation $a^2 + db^6 = c^n$, where $d > 0$ is fixed, we are able to attach a Frey $\mathbb{Q}$-curve only for the cases $d = 1$ [BC12] and 3 which makes these values special.

The paper is organised as follows. In Section 2 we recall the terminology and theory of $\mathbb{Q}$-curves. In Section 3 we attach a Frey curve to a solution (a, b, c) of (2). We prove that the Frey curve is a $\mathbb{Q}$-curve and compute its arithmetic invariants. In Section 4 we prove Theorem 1 when $n \geq 11$ is a prime using Ellenberg's analytic method [Ell04] which we explain in Section 5. In Section 6 we prove Theorem 1 for the small exponents $n = 3, 4, 5, 7$.

Date: Submitted Apr. 15, 2019; accepted Feb. 14, 2020.

2010 *Mathematics Subject Classification.* Primary 11D61.

Key words and phrases. Fermat equations, $\mathbb{Q}$-curves, Galois representations, elliptic curve Chabauty.

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. The author is also grateful to the referees for the very useful comments and suggestions.

The computations of the paper were performed in Magma [BCP97] and the programs can be found in the Bulletin's website, at the location `http://bulletin.math.uoc.gr/vol/64/2020-koutsianas/`.

2. Preliminaries

In this section we recall the main definitions of the $\mathbb{Q}$-curves and their associated Galois representations; we recommend [BC12, ES01, Que00, Rib04, Che10] for a more detailed exposition.

Let K be a number field and E/K an elliptic curve without complex multiplication such that for every $\sigma \in G_{\mathbb{Q}}$ there exists an isogeny $\mu_E(\sigma) : {}^{\sigma}E \longmapsto E$. Then, E is called a $\mathbb{Q}$-*curve defined over* K. We make a choice of the isogenies $\mu_E(\sigma)$ such that for any $\sigma, \tau \in G_{\mathbb{Q}}$ with $\sigma\mid_K = \tau\mid_K$ it holds $\mu_E(\sigma) = \mu_E(\tau)$.

We define

$$c_E(\sigma,\tau) := \mu_E(\sigma)^{\sigma}\mu_E(\tau)\mu_E(\sigma\tau)^{-1}, \in (\mathrm{Hom}(E,E)\otimes_{\mathbb{Z}}\mathbb{Q})^* = \mathbb{Q}^*, \tag{3}$$

where $\mu_E^{-1} := (1/\deg\mu_E)\mu_E^{\vee}$ and $\mu_E^{\vee}$ is the dual of μ_E. A short computation shows that the map $c_E : G_{\mathbb{Q}} \times G_{\mathbb{Q}} \to \mathbb{Q}^*$ is a 2-cocycle under the trivial action of $G_{\mathbb{Q}}$ on $\mathbb{Q}^*$. A different choice of the isogenies $\mu_E(\sigma)$ changes c_E only by a coboundary, hence c_E determines a class in $H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$ which depends only on the $\overline{\mathbb{Q}}$-isogeny class of E.

Because of the natural inclusion of $\mathbb{Q}^* \to \overline{\mathbb{Q}}^*$ the map c_E determines an element in $H^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*)$. Tate has shown that $H^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*)$ is trivial when $G_{\mathbb{Q}}$ acts trivially on $\overline{\mathbb{Q}}^*$ [Ser77, Theorem 4]. So, there exists a continuous map $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ such that

$$c_E(\sigma,\tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}, \tag{4}$$

as cocycles. The map β is called a *splitting map* of c_E. From here on, for a given splitting map β we enlarge K if necessary so that β factors through K.

We define an action of $G_{\mathbb{Q}}$ on $\overline{\mathbb{Q}}_p \otimes_{\mathbb{Z}_p} T_p(E)$ given by

$$\rho_{E,\beta,p}(\sigma)(1\otimes x) := \beta(\sigma)^{-1} \otimes \mu_E(\sigma)(\sigma(x)), \tag{5}$$

where $T_p(E)$ is the p-adic Tate module of E and $x \in T_p(E)$. From the definition of $\rho_{E,\beta,p}$ we have that $\mathbb{P}\rho_{E,\beta,p}\mid_{G_K} \simeq \mathbb{P}\phi_{E,p}$ where

$$\phi_{E,p} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_2(\mathbb{Z}_p), \tag{6}$$

is the usual Galois representation of G_K acting on $T_p(E)$ and $\mathbb{P}\rho_{E,\beta,p}$ and $\mathbb{P}\phi_{E,p}$ are the projective representations of $\rho_{E,\beta,p}$ and $\phi_{E,p}$, respectively [ES01, Proposition 2.3].

Let A be an abelian variety over K of dimension g. If there is a number field L with $[L:\mathbb{Q}] = g$ such that

$$L \hookrightarrow \mathrm{End}_K(A)\otimes\mathbb{Q},$$

then we say A is *of* GL_2*-type*. Let $T_p(A)$ be the p-adic Tate module of an abelian variety A of GL_2-type; because A is of GL_2-type, $T_p(A)$ is free of rank two as $L\otimes_{\mathbb{Z}}\mathbb{Q}_p$-modulo [Rib04, Section 2]. Suppose $\pi \mid p$ is a prime in L, then from the natural map $L\otimes_{\mathbb{Z}}\mathbb{Q}_p \to L_\pi$ we have a Galois representation of $G_{\mathbb{Q}}$

$$\rho_{A,\pi} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{L}_\pi),$$

which is the action of $G_{\mathbb{Q}}$ on the π-adic Tate module of A. Given a splitting map β, Ribet [Rib04, Section 6] attaches an abelian variety A_β over $\mathbb{Q}$ of GL_2-type such that E is a simple factor over $\overline{\mathbb{Q}}$ and $\rho_{E,\beta,p} \simeq \rho_{A_\beta,\pi}$ [ES01, Proposition 2.10].

Suppose β' is an other splitting map. From (4) it is not hard to show that there exists a character $\chi : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ such that $\beta' = \chi\beta$. On the other hand, for a given character χ the map $\beta' = \chi\beta$ is an other splitting map. The abelian varieties $A_{\beta'}$ and A_β are twists of each other with $\rho_{E,\beta',p} = \chi \otimes \rho_{E,\beta,p}$.

We recall that we have made the assumption that β factors through K. For practical purposes it is important to make a choice of β such that K has small degree. Among many others in [Que00] the author studies this problem and explains that we can make a choice of a twist E_β/K_β of E such that $c_{E_\beta}(\sigma,\tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$ as cocycles, β factors through a number field K_β and the degree of K_β is not 'big'. The field K_β is called the *splitting field of* β.

Suppose we have determined E_β/K_β. In [Rib04, Section 6] the author shows that the abelian variety A_β is a quotient of $\mathrm{Res}_{K_\beta/\mathbb{Q}} E_\beta$ over $\mathbb{Q}$, and the endomorphism algebra of A_β is equal to M_β where M_β is the field generated by the values of β.

We define the map $\epsilon : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ given by

$$\epsilon(\sigma) = \frac{\beta(\sigma)^2}{\deg \mu(\sigma)}. \tag{7}$$

Because

$$\frac{\beta^2(\sigma)\beta^2(\tau)}{\beta^2(\sigma\tau)} = c_E^2(\sigma,\tau) = \deg(\mu_E(\sigma)^\sigma \mu_E(\tau)\mu_E(\sigma\tau)^{-1}) = \frac{\deg(\mu(\sigma))\deg(\mu(\tau))}{\deg(\mu(\sigma\tau))},$$

we conclude that the map ϵ is a character. We denote by K_ϵ the field over the character ϵ factors. From the definition of $\rho_{E,\beta,p}$ we get that

$$\det(\rho_{E,\beta,p}) = \epsilon^{-1} \cdot \chi_p, \tag{8}$$

where χ_p is the p-th cyclotomic character. We can attach a residual representation associate to $\rho_{E,\beta,p}$ (see [ES01, p. 107])

$$\bar{\rho}_{E,\beta,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{F}}_p^* \,\mathrm{GL}_2(\mathbb{F}_p). \tag{9}$$

Similarly, we denote by $\bar{\phi}_{E,p}$ the residual representation associate to $\phi_{E,p}$.

A $\mathbb{Q}$-curve E is called *modular* if there is a positive integer N such that E is the quotient over $\overline{\mathbb{Q}}$ of the modular curve $J_1(N)$. If E is modular, then there is a newform $f \in S_2(\Gamma_0(N), \epsilon^{-1})$ attached to E such that A_f is defined over $\mathbb{Q}$ of GL_2-type where A_f is the *abelian variety associated to* f (see [DS05, Section 6.6] for the definition of A_f). This is because the modular curve $J_1(N)$ it is a product of A_f's up to isogeny over $\mathbb{Q}$ [Rib80, Section 2]. Then, from [Che10, Proposition 10] A_f is isogenous to A_β for some splitting map β, hence it holds $\rho_{E,\beta,p} \simeq \rho_{f,p}$ where $\rho_{f,p}$ is the Galois representation attached to f (see [DS05, Section 9.5] for the construction of $\rho_{f,p}$). Because splitting maps differ by a character we conclude that for any splitting map β there exists a newform f of $J_1(N)$ such that $\rho_{E,\beta,p} \simeq \rho_{f,p}$. Conversely, if $\rho_{E,\beta,p} \simeq \rho_{f,p}$ for some newform $f \in S_2(\Gamma_0(N), \epsilon^{-1})$, then A_β is isogenous to A_f over $\mathbb{Q}$ so E is a quotient of $J_1(N)$.

Assuming the Serre's modularity conjecture [Ser87] Ribet proves that any $\mathbb{Q}$-curve is modular [Rib04, Corollary 6.2]. Nowadays, Serre's modularity conjecture is a theorem [KW09a, KW09b, Kis09].

Theorem 2. *Suppose E/K is a $\mathbb{Q}$-curve. Then, E is modular.*

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

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 $n = p$ be an odd prime. We define

$$E_{a,b} : Y^2 = X^3 - 9\sqrt{-3}b(4a - 5\sqrt{-3}b^3)X + 18(2a^2 - 14\sqrt{-3}ab^3 - 33b^6). \tag{10}$$

When it is not confusing we use the notation E instead of $E_{a,b}$. The invariants of E are given by

$$j(E) = 2^4 \cdot 3^3 \cdot \sqrt{-3} \cdot b^3 \cdot \frac{(4a - 5\sqrt{-3}b^3)^3}{(a + \sqrt{-3}b^3)^3 \cdot (a - \sqrt{-3}b^3)}, \tag{11}$$

$$\Delta(E) = -2^8 \cdot 3^7 \cdot (a - \sqrt{-3}b^3) \cdot (a + \sqrt{-3}b)^3, \tag{12}$$

$$c_4(E) = 2^4 \cdot 3^3 \cdot \sqrt{-3} \cdot b \cdot (4a - 5\sqrt{-3}b^3), \tag{13}$$

$$c_6(E) = -2^6 \cdot 3^5 \cdot (2a^2 - 14\sqrt{-3}b^3a - 33b^6). \tag{14}$$

We are grateful to the referees for mentioning this shorter proof of the next lemma.

Lemma 3.1. *If (a, b, c) is a primitive solution of (2), then the curve E does not have complex multiplication.*

Proof. From (11), $j(E) \in \mathbb{Q}(\sqrt{-3})$ and an easy symbolic computation shows that, in $j(E)$, the coefficient of $\sqrt{-3}$ is

$$864ab^3 \frac{(2a^2 - 75b^6)(16a^2 - 33b^6)}{(a^2 + 3b^6)^3},$$

which is non-zero because a and b are non-zero integers. In particular, $j(E) \notin \mathbb{R}$ which, by the theory of complex multiplication [Sil94, Ch. II, problem 2.9], implies that E is not a CM-curve. □

Remark. It is important to mention that the trivial solution $(\pm 1, 0, 1)$ corresponds to an elliptic curve E with complex multiplication. Because of Lemma 3.1 this obstruction has been isolated.

Lemma 3.2. *Let (a, b, c) be a primitive solution of (2), then c is divisible by a prime different from 2 and 3.*

Proof. Because (a, b, c) is a primitive solution of $a^2 + 3b^6 = c^p$ we have that $3 \nmid c$. Because $p \geq 3$ and $a^2 + 3b^6 \not\equiv 0 \pmod 8$ we have that $2 \nmid c$. □

Because of Lemma 3.1 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 $\mu(\sigma) : {}^{\sigma}E \longmapsto E$ such that $\mu(\sigma) = 1$ for $\sigma \in G_K$ and $\mu(\sigma)$ equals the 3-isogeny above for $\sigma \notin G_K$.

Let d be the *degree map* (see [Que00, p. 289]), then we have that $d(G_{\mathbb{Q}}) = \{1, 3\} \subset \mathbb{Q}^*/\mathbb{Q}^{*2}$. 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, p. 294]. We can see that the quaternion algebra $(-3, 3)$ is unramified and so $\epsilon = 1$, $K_\epsilon = \mathbb{Q}$ and $K_\beta = \mathbb{Q}(\sqrt{-3})$. Moreover, we have $\beta(\sigma) = \sqrt{d(\sigma)}$ and so $M_\beta = \mathbb{Q}(\sqrt{3})$.

Let $A_\beta = \mathrm{Res}_{K/\mathbb{Q}} E$. Since $K_\beta = K$ we understand that $\xi_K(E)$ has trivial Schur class, where $\xi_K(E)$ is as in [Que00, p. 288]. Thus, from [Que00, Theorem 5.4] we have that A_β is a GL_2-type variety with $\mathbb{Q}$-endomorphism algebra isomorphic to M_β. Moreover, from the definition of $\rho_{E,\beta,p}$ we understand that $\rho_{E,\beta,p} \mid_{G_K} \simeq \phi_{E,p}$.

Let $\mathfrak{p}_2$ and $\mathfrak{p}_3$ be the primes in K above 2 and 3, respectively; thus $\mathfrak{p}_2 = \langle 2 \rangle$ and $\mathfrak{p}_3 = \langle \sqrt{-3} \rangle$.

Lemma 3.3. *The elliptic curve E is a minimal model with conductor equal to*

$$N(E) = \mathfrak{p}_2^2 \cdot \mathfrak{p}_3^8 \cdot \prod_{\mathfrak{p}|c} \mathfrak{p}. \tag{15}$$

Proof. Suppose $\mathfrak{p}$ is a prime in K with $\mathfrak{p} \mid \Delta(E)$. If $\mathfrak{p}$ does not divide 2 and 3, or equivalently $\mathfrak{p} \mid c$ by Lemma 3.2, we understand from (13) that $\mathfrak{p} \nmid c_4(E)$, hence E has multiplicative reduction at $\mathfrak{p}$ [Sil86, Ch. VII, Proposition 5.1].

For $\mathfrak{p} = \mathfrak{p}_3$ or $\mathfrak{p}_2$ it is more convenient to use the following isomorphic to (10) model of E

$$E : Y^2 + 6\sqrt{-3}bXY - 12(\sqrt{-3}b^3 + a)Y = X^3. \tag{16}$$

Suppose $\mathfrak{p} = \mathfrak{p}_3$. From Tate's algorithm we can prove that E has IV^* reduction type and because $v_{\mathfrak{p}_3}(\Delta) = 14$ the exponent of the conductor at $\mathfrak{p}_3$ is equal to 8.

Suppose $\mathfrak{p} = \mathfrak{p}_2$. Again, we apply Tate's algorithm and we prove that E has IV^* reduction type. Because $v_{\mathfrak{p}_2}(\Delta(E)) = 8$ we have the result. □

Lemma 3.4. *The conductor of A_β is*

$$d_{K/\mathbb{Q}}^2 \cdot \mathrm{Norm}_{K/\mathbb{Q}}(N(E)) = 2^4 \cdot 3^{10} \cdot \prod_{p|c} p^2. \tag{17}$$

Proof. This is an immediate consequence of [Mil72, Proposition 1] and the fact that K is unramified outside 3. □

Since A_β is of GL_2-type with $M_\beta = \mathbb{Q}(\sqrt{3})$, the conductor N_{A_β} of $\rho_{E,\beta,p}$ is given by

$$N_{A_\beta} = 2^2 \cdot 3^5 \cdot \prod_{p|c} p, \tag{18}$$

as it is explained in [Che10, Lemma 29].

In the modular method we do not use $\rho_{E,\beta,p}$, which has conductor depending on the solutions, but we work with the residual representation $\bar{\rho}_{E,\beta,p}$. We have to compute the Serre invariants $N_{\bar{\rho}} = N(\bar{\rho}_{E,\beta,p})$, $k_{\bar{\rho}} = k(\bar{\rho}_{E,\beta,p})$ and $\epsilon_{\bar{\rho}} = \epsilon(\bar{\rho}_{E,\beta,p})$ of $\bar{\rho}_{E,\beta,p}$ [Ser87, KW09a] and prove that $\bar{\rho}_{E,\beta,p}$ is irreducible. Because K is unramified away from 3 for $p \neq 3$ it holds $I_p \subset G_K$ where I_p is an inertia group at p.

Proposition 3.5. *The representation $\bar{\phi}_{E,p}\,|_{I_p}$ is finite flat for $p \neq 2, 3$.*

Proof. Let $\mathfrak{p}$ be a prime above p. By Lemma 3.3 we know that E has good or multiplicative reduction at $\mathfrak{p}$. In the case of multiplicative reduction the exponent of $\mathfrak{p}$ in the minimal discriminant of E is divisible by p. As we have mentioned $I_p \subset G_K$ and the result follows as it is explained in [DDT97, Proposition 2.12]. □

Proposition 3.6. *The representation $\bar{\phi}_{E,p}\,|_{I_\ell}$ is trivial for $\ell \neq 2, 3, p$.*

Proof. Let $\mathfrak{l}$ be a prime above ℓ. Because of Lemma 3.3 we know that E has good or multiplicative reduction at $\mathfrak{l}$. In the case of multiplicative reduction the exponent of $\mathfrak{l}$ in the minimal discriminant of E is divisible by p. As we have mentioned $I_p \subset G_K$ and the result follows as it is explained in [DDT97, Proposition 2.12]. □

Proposition 3.7. *Suppose $p \neq 2, 3$. Then $N_{\bar{\rho}} = 972$.*

Proof. Because we want to compute the Artin conductor of $\bar{\rho}_{E,\beta,p}$, we consider only ramification at primes above $\ell \neq p$. We recall that $\rho_{E,\beta,p}\,|_{G_K} \simeq \phi_{E,p}$.

Let consider $\ell \neq 2, 3, p$. We recall that $K = K_\beta$. Because $\ell \neq 3$ we have that K_β is unramified at ℓ, so $I_\ell \subset G_K$. Because $\bar{\rho}_{E,\beta,p}|_{G_K} \simeq \bar{\phi}_{E,p}$ and $\bar{\phi}_{E,p}\,|_{I_\ell}$ is trivial from Proposition 3.6 we have that $\bar{\rho}_{E,\beta,p}$ is trivial at I_ℓ. Thus, $\bar{\rho}_{E,\beta,p}$ is unramified outside $2, 3, p$.

Suppose $\ell = 2, 3$. From (11) we understand that E has potential good reduction at primes above $2, 3$. That means $\phi_{E,p}|_{I_\ell}$ factors through a finite group of order divisible only by $2, 3$ [Kra90, p. 354]. Thus, $\rho_{E,\beta,p}|_{I_\ell}$ factors through a finite group of order divisible only by $2, 3$. It follows that the exponent of ℓ in the conductor of $\bar{\rho}_{E,\beta,p}$ is the same as in the conductor of $\rho_{E,\beta,p}$ as $p \neq 2, 3$. □

Proposition 3.8. *Suppose $p \neq 2, 3$. Then $k_{\bar{\rho}} = 2$.*

Proof. The weight is determined by $\bar{\rho}_{E,\beta,p}|_{I_p}$. For $p \neq 3$ we recall that $I_p \subset G_K$. Because $\bar{\rho}_{E,\beta,p}|_{G_K} \simeq \bar{\phi}_{E,p}$, $\bar{\phi}_{E,p}\,|_{I_p}$ is finite flat from Proposition 3.5, and the determinant of $\bar{\phi}_{E,p}$ is the cyclotomic p-th character then from [Ser87, Prop. 4] we have the conclusion. □

Proposition 3.9. *The character $\epsilon_{\bar{\rho}}$ is trivial.*

Proof. This is a consequence of the fact that ϵ is trivial and equation (8). □

From [Ell04, Proposition 3.2] and Lemma 3.2 we have.

Proposition 3.10. *Let assume that $\bar{\rho}_{E,\beta,p}$ is reducible for $p \neq 2, 3, 5, 7, 13$. Then E has potentially good reduction at all primes above $\ell > 3$.*

An immediate consequence of Proposition 3.10 and Lemma 3.2 is the following.

Corollary 3.11. *The representation $\bar{\rho}_{E,\beta,p}$ is irreducible for $p \neq 2, 3, 5, 7, 13$.*

Proposition 3.12. *If $p = 13$, then $\bar{\rho}_{E,\beta,p}$ is irreducible.*

Proof. This is similar to [BC12, Proposition 17] which is based on results in [Ken79] about $\mathbb{Q}$-rational points on $X_0(39)/w_3$. □

4. Proof of Theorem 1

Suppose f is a newform of weight 2, level N_f and trivial character with q-expansion

$$f(q) = 1 + \sum_{n \geq 2} a_n(f) q^n.$$

We denote by K_f the *eigenvalue field* of f and we say f is *rational* if $[K_f : \mathbb{Q}] = 1$ and *irrational*, otherwise. Suppose p is a rational prime and $\mathfrak{p}$ a prime ideal of K_f above p. Then, we can associate a continuous, semisimple representation

$$\bar{\rho}_{f,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p),$$

that is unramified at all primes $q \nmid pN_f$ and $\mathrm{Tr}(\bar{\rho}_{f,p}(\mathrm{Frob}_q)) \equiv a_q(f) \pmod{\mathfrak{p}}$, where Frob_q is a Frobenius element at q.

Proposition 4.1. *Let f be a newform of weight 2, level N_f and trivial character. Suppose $\bar{\rho}_{E,\beta,p} \simeq \bar{\rho}_{f,p}$. Let $q \neq p$ be a rational prime with $q \nmid N_f N(E)$. We define*

$$B(q,f) = \begin{cases} N(a_q(E) - a_q(f)), & \text{if } a^2 + 3b^6 \not\equiv 0 \pmod{q} \text{ and } \left(\frac{-3}{q}\right) = 1, \\ N(a_q(f)^2 - a_{q^2}(E) - 2q), & \text{if } a^2 + 3b^6 \not\equiv 0 \pmod{q} \text{ and } \left(\frac{-3}{q}\right) = -1, \\ N((q+1)^2 - a_q(f)^2), & \text{if } a^2 + 3b^6 \equiv 0 \pmod{q}. \end{cases}$$

where $a_{q^i}(E)$ is the trace of Frob_q^i *acting on the Tate module $T_p(E)$. Then $p|B(q,f)$.*

Proof. From Section 3 we recall that $A_\beta = \mathrm{Res}_{K/\mathbb{Q}}(E)$ and $M_\beta = \mathbb{Q}(\sqrt{3})$. Let π be a prime of M_β above p. As we mentioned in Section 2 we have that $\rho_{A_\beta,\pi} = \rho_{E,\beta,p}$ We recall that

$$\rho_{E,\beta,p}(\sigma)(1\otimes x) = \beta(\sigma)^{-1}\otimes \mu(\sigma)(\phi_{E,p}(\sigma)(x)), \tag{19}$$

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 $\bar\rho_{A_\beta,\pi} = \bar\rho_{E,\beta,p} \simeq \bar\rho_{f,p}$ and $\beta(\sigma) = \sqrt{d(\sigma)}$.

Let assume the case $a^2+3b^6 \equiv 0 \pmod q$. By (18) we have that $q \parallel N_{A_\beta}$ and from [Car86, Théorèm (A)], [DDT97, Theorem 3.1] we have that

$$p \mid N(a_q(f)^2 - (q+1)^2). \tag{20}$$

For the rest of the proof we assume that $a^2+3b^6 \not\equiv 0 \pmod q$. When $\left(\frac{-3}{q}\right) = 1$ we have that $\sigma = \mathrm{Frob}_q \in G_K$, $\mu(\sigma) = 1$ and $d(\sigma) = 1$, so $\mathrm{Tr}\,\bar\rho_{A_\beta,\pi}(\sigma) = \mathrm{Tr}\,\bar\phi_{E,p}(\sigma)$. Because $\bar\rho_{A_\beta,\pi} = \bar\rho_{E,\beta,p} \simeq \bar\rho_{f,p}$ we conclude that $a_q(E) \equiv a_q(f) \pmod\pi$ and so $p \mid N(a_q(E) - a_q(f))$.

Suppose $\left(\frac{-3}{q}\right) = -1$, then $\sigma = \mathrm{Frob}_q \notin G_K$. Because $\sigma^2 \in G_K$ and similarly to the above lines we have that $\mathrm{Tr}\,\bar\rho_{A_\beta,\pi}(\sigma^2) = \mathrm{Tr}\,\bar\phi_{E,p}(\sigma^2) = a_{q^2}(E)$. We know that

$$\frac{1}{\det(I-\bar\rho_{A_\beta,\pi}(\sigma)q^{-s})} = \exp\sum_{n=1}^{\infty}\mathrm{Tr}\,\bar\rho_{A_\beta,\pi}(\sigma^n)\frac{q^{-ns}}{n} = \frac{1}{1-\mathrm{Tr}\,\bar\rho_{A_\beta,\pi}(\sigma)q^{-s}+qq^{-2s}} \tag{21}$$

From the coefficient of q^{-2s} we have that $\mathrm{Tr}\,\bar\rho_{A_\beta,\pi}(\sigma^2) = \mathrm{Tr}\,\bar\rho_{A_\beta,\pi}(\sigma)^2 - 2q$. As above we conclude that $a_q(f)^2 \equiv a_{q^2}(E) + 2q \pmod\pi$, so $p \mid N(a_q(f)^2 - a_{q^2}(E) - 2q)$. □

The value of $B(q,f)$ depends on the residue classes of (a,b). So, with the notation of Proposition 4.1 we define

$$C(q,f) = q\cdot \prod_{\substack{a,b\in\mathbb{F}_q,\\(a,b)\neq(0,0)}} B(q,f).$$

Proof of Theorem 1. Let assume that $p \geq 11$ is an odd prime and (a,b,c) a primitive solution of (2). We attach to (a,b,c) the Frey $\mathbb{Q}$-curve E with β as in Section 3. From Corollary 3.11 and Proposition 3.12 the representation $\bar\rho_{E,\beta,p}$ is irreducible, hence by Serre's modularity conjecture [KW09a, Theorem 1.1] $\bar\rho_{E,\beta,p}$ is modular. Thus, there exists a newform $f \in S_{k_{\bar\rho}}(N_{\bar\rho},\epsilon_{\bar\rho})$ such that $\bar\rho_{E,\beta,p} \simeq \bar\rho_{f,p}$. From Propositions 3.7, 3.8 and 3.9 we conclude that $f \in S_2(\Gamma_0(972))$

There are 7 newforms of level 972. Four of them are rational with complex multiplication by $\mathbb{Q}(\sqrt{-3})$ and the remaining are irrational. In Section 5 we show how we can prove that non solutions arise from the rational newforms for $p \geq 11$ using Ellenberg's analytic method, see Proposition 5.5. For the irrational newforms we apply Proposition 4.1. It is enough to compute $\gcd_{q\leq 30}(C(q,f))$ with $q \neq 2,3$ to prove that $p \leq 7$ (see *CongruenceCriterion.m*). □

5. Eliminating the CM forms

In this section we explain and apply the method of Ellenberg [Ell04] which allows us to prove that no solutions of (2) arise from the rational newforms for $p \geq 11$.

Proposition 5.1 (Proposition 3.4 [Ell04])**.** *Let K be an imaginary quadratic field and E/K a $\mathbb{Q}$-curve of squarefree degree d. Suppose the image of $\mathbb{P}\bar\rho_{E,\beta,p}$ lies in the normalizer of a split*

Cartan subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$*, 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 [Ell04])**.** *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* $\mathbb{P}\bar{\rho}_{E,\beta,p}$ *lies in the normalizer of a non-split Cartan subgroup of* $\mathrm{PGL}_2(\mathbb{F}_p)$ *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 for which Proposition 5.3 holds.

Proposition 5.3 (Proposition 3.9 [Ell04])**.** *Let* K *be an imaginary quadratic field and* χ_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* $w_p f = f$ *and* $w_d f = -f$*,*
- *a newform in* $S_2(\Gamma(d'p^2))$ *with* d' *a proper divisor of* d *and* $w_p f = f$

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

The reason why Proposition 5.3 implies Proposition 5.2 is explained in [Ell04, p. 775]. Before we show how we can prove when Proposition 5.3 holds we need to introduce some notation.

Let f be a modular form with q-expansion

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

We define $L_\chi(f) := L(f \otimes \chi, 1)$ where χ is a Dirichlet character. We can think a_m and L_χ 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 we define

$$(a_m, L_\chi)_N := \sum_{f\in\mathcal{F}} a_m(f) L_\chi(f) \tag{23}$$

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

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

In [Ell04] it is explained that Proposition 5.3 holds as long as $|(a_1, L_\chi)_{p^2}^{p-\mathrm{new}}| > 0$.

In our case we have $d = 3$ and $\chi = \chi_{-3} = \left(\frac{-3}{n}\right)$ while $\mathrm{cond}(\chi_{-3}) = 3$. So we have the following.

Proposition 5.4. *Let* $p \geq 11$ *be a prime. Then there exists a newform* $f \in S_2(\Gamma_0(p^2))$ *such that* $w_p f = f$ *and* $L(f \otimes \chi_{-3}) \neq 0$*.*

Proof. In [DU09, Lemma8] the authors prove that $|(a_1, L_\chi)^{p-\mathrm{new}}| > 0$ for $p \geq 137$. For $p < 137$ we have written a Magma program which proves that the same it true for $11 \leq p < 137$ (see *NewformTwist.m*). □

Proposition 5.5. *Let* $p \geq 11$ *be a prime. Then, no primitive solutions of* (2) *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 $\bar{\rho}_{f,p}$ lies in the normalizer of a Cartan group (either split or non-split) [BS04, Section 4.4].

Suppose $\bar{\rho}_{f,p}$ lies in the normalizer of a non-split Cartan group. Because $\bar{\rho}_{f,p} \simeq \bar{\rho}_{E,\beta,p}$ we understand that $\mathbb{P}\bar{\rho}_{E,\beta,p}$ also lies in the normalizer of a non-split Cartan group. For $c \neq 1$ and Lemma 3.3 we conclude that there exists a prime $\mathfrak{p}$ in K, not dividing 2 and 3, such that E has multiplicative reduction at $\mathfrak{p}$. From Proposition 5.4 we understand that Proposition 5.3 holds for $p \geq 11$ which implies that Proposition 5.2 also holds for $p \geq 11$. However, this is a contradiction to the fact that E has multiplicative reduction at $\mathfrak{p}$.

Suppose $\bar{\rho}_{f,p}$ lies in the normalizer of a split Cartan group. Because $\bar{\rho}_{f,p} \simeq \bar{\rho}_{E,\beta,p}$ we understand that $\mathbb{P}\bar{\rho}_{E,\beta,p}$ also lies in the normalizer of a split Cartan group. For $c \neq 1$ and Lemma 3.3 we conclude that there exists a prime $\mathfrak{p}$ in K, not dividing 2 and 3, such that E has multiplicative reduction at $\mathfrak{p}$. However, from Propositions 5.1 this is not possible for $p \geq 11$ and $p \neq 13$. For $p = 13$ Proposition 5.1 does not hold. However, the argument following [Ell04, Proposition 3.9] also works for the split case (see also [BEN10, Proposition 6]). So, from Proposition 5.4 we have the result. □

6. Solutions for $n = 3, 4, 5, 7$

In this final section we prove Theorem 1 for $n = 3, 4, 5, 7$. We need the following lemma.

Lemma 6.1. *Let $p \geq 5$ be an odd prime and x, y, z pairwise coprime integers such that $x^2 + 3y^2 = z^p$. We define*

$$f_1(u,v) = \sum_{i=0}^{\frac{p-1}{2}} \binom{p}{2i+1} (-3)^{\frac{p-1}{2}-i} u^{2i+1} v^{p-1-2i}, \tag{25}$$

$$f_2(u,v) = \sum_{i=0}^{\frac{p-1}{2}} \binom{p}{2i} (-3)^{\frac{p-1}{2}-i} u^{2i} v^{p-2i}. \tag{26}$$

Then there exist integers u_0, v_0 with $(u_0, v_0) = 1$ such that $x = f_1(u_0, v_0)$, $y = f_2(u_0, v_0)$ and $z = u_0^2 + 3v_0^2$.

Proof. Because $p \geq 5$ and x, y, z are pairwise coprime we understand that $(z, 6) = 1$. The ring of integers of $K = \mathbb{Q}(\sqrt{-3})$ is $\mathbb{Z}[\omega]$ where $\omega = \frac{1+\sqrt{-3}}{2}$. We know that K has class number one and the only units in $\mathbb{Z}[\omega]$ are the 6-th roots of unity which are powers of $-\omega$. Factorizing $x^2 + 3y^2 = z^p$ over K we have

$$(x + y\sqrt{-3})(x - y\sqrt{-3}) = z^p. \tag{27}$$

Because $(z, 6) = 1$ and the order of the roots of unity is 6 coprime to p, we understand that there exist $u_0', v_0' \in \mathbb{Z}$ such that

$$x + y\sqrt{-3} = \left(\frac{u_0' + v_0'\sqrt{-3}}{2}\right)^p,$$

where u_0' and v_0' have the same parity. Suppose that $u_0' \equiv v_0' \equiv 1 \pmod 2$, then we have

$$z^p = x^2 + 3y^2 = \left(\frac{u_0'^2 + 3v_0'^2}{2}\right)^p,$$

and we conclude that $2z = u_0'^2 + 3v_0'^2$. Because $2 \nmid z$ and taking the last equation $\pmod 4$ we get a contradiction, hence $u_0' \equiv v_0' \equiv 0 \pmod 2$. Suppose $u_0' = 2u_0$ and $v_0' = 2v_0$, then

$$x + y\sqrt{-3} = \left(u_0 + v_0\sqrt{-3}\right)^p.$$

Because $(x, y) = 1$ we have that $(u_0, v_0) = 1$. After expanding the right-hand side of the above equation we get

$$x = \sum_{i=0}^{\frac{p-1}{2}} \binom{p}{2i+1} (-3)^{\frac{p-1}{2}-i} u_0^{2i+1} v_0^{p-1-2i},$$

$$y = \sum_{i=0}^{\frac{p-1}{2}} \binom{p}{2i} (-3)^{\frac{p-1}{2}-i} u_0^{2i} v_0^{p-2i}.$$

□

Let (a, b, c) be a primitive solution of (2).

6.1. **Case** $n = 3$**:** A solution with $b \neq 0$ corresponds to a rational point of the elliptic curve $E : y^2 = x^3 - 3$ via the equation

$$\left(\frac{a}{b^3}\right)^2 = \left(\frac{c}{b^2}\right)^3 - 3. \tag{28}$$

The curve E is Cremona's curve with label 972B1 which has trivial Mordell-Weil group [Cre97], hence there are no solutions of (2) for $n = 3$.

6.2. **Case** $n = 4$**:** We recall that $2 \mid b$. Equation (2) is written

$$(c^2 + a)(c^2 - a) = 3(b^3)^2.$$

From elementary number theory we have that there exist $r, s \in \mathbb{Z}$ such that $\pm a = r^2 - 3s^2$, $b^3 = 2rs$ and $c^2 = r^2 + 3s^2$ with $(r, s) = 1$, r odd and s even. Then, $r = R^3$, $s = 4S^3$ and $c^2 = R^6 + 48S^6$, which means that the point $(R/S, c/S^3)$ is a rational point on the curve $C : Y^2 = X^6 + 1$. In [BT11] the authors have computed the rational points of C and it holds $C(\mathbb{Q}) = \{\infty^{\pm}, (\pm 1, \pm 7)\}$. From $C(\mathbb{Q})$ it is easy to compute the solutions of (2) for $n = 4$.

6.3. **Case** $n = 5$**:** For the case $n = 5$ we are grateful to the referees for this shorter proof. From Lemma 6.1 we have that there exist coprime integers u, v such that $b^3 = f_2(u, v) = v(5u^4 - 30u^2v^2 + 9v^4)$. Thus we can conclude that there exist coprime b_1, b_2 with $b_1 b_2 \neq 0$ such that

$$\begin{cases} v = 5^2 \cdot b_1^3 \\ 5u^4 - 30u^2v^2 + 9v^4 = 5 \cdot b_2^3 \end{cases} \quad \text{or} \quad \begin{cases} v = b_1^3 \\ 5u^4 - 30u^2v^2 + 9v^4 = b_2^3 \end{cases}$$

For the first case and after a straightforward combination of the two equations we get

$$(u^2 - 1875b_1^6)^2 = b_2^3 + 2^2 3^2 5^7 b_1^{12}. \tag{29}$$

This means that the point $(X, Y) = \left(b_2/b_1^4, (u^2 - 1875b_1^6)/b_1^6\right)$, because $b_1 \neq 0$, is a rational point of the elliptic curve $Y^2 = X^3 + 2^2 3^2 5^7$. However, this curve has trivial Mordell-Weil group.

For the second case and similar to the previous case we get

$$(25u^2 - 75b_1^6)^2 = (5b_2)^3 + 4500b_1^{12}. \tag{30}$$

Then, because $b_1 \neq 0$ the point $(X, Y) = (5b_2/b_1^4, (25u^2 - 75b_1^6)/b_1^6)$ is a rational point of the elliptic curve $Y^2 = X^3 + 4500$, whose Mordell-Weil group is trivial.

From the above we conclude that there are not solutions of (2) for $n = 5$.

6.4. **Case $n = 7$:** From Lemma 6.1 we have that there exist coprime integers u, v such that $b^3 = f_2(u, v) = v(7u^6 - 105u^4v^2 + 189u^2v^4 - 27v^6)$. Thus we can conclude that there exist coprime b_1, b_2 with $b_1b_2 \neq 0$ such that

$$\begin{cases} v = 7^2b_1^3 \\ 7u^6 - 105u^4v^2 + 189u^2v^4 - 27v^6 = 7b_2^3 \end{cases} \quad \text{or} \quad \begin{cases} v = b_1^3 \\ 7u^6 - 105u^4v^2 + 189u^2v^4 - 27v^6 = b_2^3 \end{cases}$$

From Lemma 6.1 we also have $a = f_1(u, v) = u^7 - 63u^5v^2 + 315u^3v^4 - 189uv^6$ and $c = u^2 + 3v^2$. Because $3 \nmid a$ we also understand that $3 \nmid u$. Moreover, it holds $2 \nmid c$ which shows that u and v have different parity.

Let $K = \mathbb{Q}(\theta)$ where $\theta^3 - \theta^2 - 2\theta + 1 = 0$. The extension $K/\mathbb{Q}$ is Galois and it holds

$$7u^6 - 105u^4v^2 + 189u^2v^4 - 27v^6 = 7\prod_{i=1}^{3}(u^2 - v^2\rho_i), \tag{31}$$

where

$$\rho_1 = \frac{-36\theta^2 + 24\theta + 87}{7},$$
$$\rho_2 = \frac{12\theta^2 - 36\theta + 27}{7},$$
$$\rho_3 = \frac{24\theta^2 + 12\theta - 9}{7}.$$

Let $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_7$ be the unique primes of K above 2, 3 and 7, respectively. We also have that 7 is the only ramified prime in K. It holds that $v_{\mathfrak{p}}(\rho_i) \geq 0$ for any prime ideal $\mathfrak{p} \neq \mathfrak{p}_7$. Because

$$\mathrm{Res}\left(u^2 - v^2\rho_1, \prod_{i=2}^{3}(u^2 - v^2\rho_i); u\right) = \frac{186624\theta^2 - 414720\theta + 165888}{49}v^8,$$
$$\mathrm{Res}\left(u^2 - v^2\rho_1, \prod_{i=2}^{3}(u^2 - v^2\rho_i); v\right) = \frac{186624\theta^2 - 414720\theta + 165888}{49}u^8,$$

we understand that

$$\langle u^2 - \rho_1 v^2 \rangle = \mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}\mathfrak{p}_7^{e_7}\mathfrak{I}^3,$$

where $0 \leq e_i < 3$ and $\mathfrak{I}$ is a fractional ideal of K with $v_{\mathfrak{p}}(\mathfrak{I}) \geq 0$ for any prime ideal $\mathfrak{p} \neq \mathfrak{p}_7$.

Because u, v have different parity and $v_{\mathfrak{p}_2}(\rho_1) = 0$ we understand that $e_2 = 0$. Moreover, it holds $v_{\mathfrak{p}_3}(\rho_1) = 1$ and $v_{\mathfrak{p}_3}(\mathfrak{I}) \geq 0$, because $3 \nmid u$ we get that $e_3 = 0$. Finally, the class number of K is one; hence we understand that there exists $d_1 \in K(S, 3)$ and $\gamma \in K^*$ such that

$$u^2 - \rho_1 v^2 = d_1\gamma^3, \tag{32}$$

where $K(S, 3) = \{x \in K^*/K^{*3} | v_{\mathfrak{p}}(x) \equiv 0 \pmod 3,\ \mathfrak{p} \notin S\}$ is the 3-Selmer group of K for $S = \{\mathfrak{p}_7\}$. We know that this is a finitely generated abelian group [Coh00, Section 7.4]. Because $v = a^2b_1^3$ with $a = 1, 7$ we get

$$u^2 - \rho_1 a^4 b_1^6 = d_1\gamma^3. \tag{33}$$

From the last equation we understand that the point $(d_1\gamma/b_1^2, ud_1/b_1^2)$ is a K-point on the elliptic curve

$$E : Y^2 = X^3 + \rho_1 d_1^2 a^4. \tag{34}$$

For all possible elements $d_1 \in K(S, 3)$ Magma is able to compute the Mordell-Weil group of $E(K)$ and it holds $\text{rank}(E(K)) \leq 2$. Because $[K : \mathbb{Q}] = 3$ and we want to compute the points $(X, Y) \in E(K)$ such that $Y/d_1 \in \mathbb{Q}$, we can apply the elliptic curve Chabauty method [Bru03] (see also [BT04, Section 4] for a nice exposition of the method). Magma has an implementation of elliptic curve Chabauty method and we have used it to prove that there are no points $(X, Y) \in E(K)$ with $Y/d_1 \in \mathbb{Q}$ (see *Exponent7.m*). Hence, there are no solutions of (2) for $n = 7$.

References

[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.

[BCP97] 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 $a^4+2^\delta b^2 = c^n$. *Int. J. Number Theory*, 06(02):311–338, 2010.

[Bru03] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[BS04] Michael A. Bennett and Chris M. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004.

[BT04] A. Bremner and N. Tzanakis. Lucas sequences whose 12th or 9th term is a square. *Journal of Number Theory*, 107(2):215 – 227, 2004.

[BT11] Andrew Bremner and Nikos Tzanakis. On the equation $Y^2 = X^6 + k$. *Ann. Sci. Math. Québec*, 35(2):153–174, 2011.

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

[Che10] Imin Chen. On the equation $a^2 + b^{2p} = c^5$. *Acta Arith.*, 143(4):345–375, 2010.

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Cre97] John Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 2nd edition, 1997.

[DDT97] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140. Int. Press, Cambridge, MA, 1997.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[DU09] Luis Dieulefait and J. Jiménez Urros. Solving Fermat-type equations via modular $\mathbb{Q}$-curves over polyquadratic fields. *J. reine angew. Math.*, 2009.

[Ell04] Jordan Ellenberg. Galois representations attached to $\mathbb{Q}$–curves and the generalized Fermat equation $a^4 + b^2 = c^p$. *American Journal of Mathemarics*, 126(4):763–787, 2004.

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

[Ken79] M. A. Kenku. The modular curve $x_0(39)$ and rational isogeny. *Math. Proc. Camb. Phil. Soc.*, 85(1):21–23, 1979.

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

[Kra90] Alain Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta Math.*, 69(4):353–385, 1990.

[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.

[Que00] Jordi Quer. $\mathbb{Q}$–curves and abelian varieties of GL_2–type. *Proc. London Math. Soc.*, 81(2):285–317, 2000.

[Rib80] Kenneth A. Ribet. Twists of modular forms and endomorphisms of abelian varieties. *Math. Ann.*, 253(1):43–62, 1980.

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

[Ser77] J.-P. Serre. Modular forms of weight one and Galois representations. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 193–268, 1977.

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

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

Department of Mathematics, The University of British Columbia, 1984 Mathematics Road Vancouver, BC, Canada

Email address: akoutsianas@math.ubc.ca