arXiv:1805.07127v4 [math.NT] 14 Apr 2019

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

ANGELOS KOUTSIANAS

Abstract. In this paper, 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 of the form

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

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

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

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

is $(a, b, c, n) = (\pm 47, \pm 2, \pm 7, 4)$. A solution (a, b, c) is called primitive if a, b, c are pairwise coprime integers and $ab \neq 0$.

For the proof of Theorem 1 we use the recent proof of modularity of $\mathbb{Q}$-curves as a result of the proof 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 $a^2 + db^6 = c^n$ and fix $d > 0$ 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 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 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 $n = 3, 4, 5, 7$. Finally, in Appendix 7 we compute the rational points of the curve $Y^2 = X^6 + 48$ which we need for the case $n = 4$.

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/`.

Date: April 16, 2019.
2010 *Mathematics Subject Classification.* Primary 11D61.
Key words and phrases. Fermat equations, $\mathbb{Q}$-curves, Galois representations.

2. Preliminaries

In this 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 $\sigma \in G_{\mathbb{Q}}$ 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 above such that μ_E is locally constant.

Let

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

where $\mu_E^{-1} := (1/\deg\mu_E)\mu_E^{\vee}$ and $\mu_E^{\vee}$ is the dual of μ_E. Thus 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. 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

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

The map β is called a *splitting map* of c_E.

We define an action of $G_{\mathbb{Q}}$ on $\overline{\mathbb{Q}}_p \otimes_{\mathbb{Z}_p} T_pE$ given by

$$\hat{\rho}_{E,p}(\sigma)(1\otimes x) = \beta(\sigma)^{-1}\otimes\mu(\sigma)(\sigma(x)) \tag{5}$$

From the definition of $\hat{\rho}_{E,p}$ we have that $\mathbb{P}\hat{\rho}_{E,p}\mid_{G_K} \simeq \mathbb{P}\hat{\phi}_{E,p}$ where

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

is the usual Galois representation attached to the p-adic Tate module of E (see [ES01, Proposition 2.3]). Given a splitting map β, Ribets [Rib04] attaches an abelian variety A_β over $\mathbb{Q}$ of GL_2-type such that E is a simple factor over $\overline{\mathbb{Q}}$.

From the definition of $\hat{\rho}_{E,p}$ we understand that the representation depends on β. Let M_β be the field generated by the values of β. We want to make a choice of β 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 $H^2(G_{\mathbb{Q}},\overline{\mathbb{Q}}^*)$. Then we choose a twist E_β/K_β such that $c_{E_\beta}(\sigma,\tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$ as cocycles and let K_β be the field over β factors which is called the *splitting field of* β. In this case, the abelian variety A_β is a quotient of $\mathrm{Res}_{K_\beta/\mathbb{Q}} E_\beta$ over $\mathbb{Q}$. The endomorphism algebra of A_β is equal to M_β and the representation on the π^n-torsion points of A_β coincides with the representation $\hat{\rho}_{E,p}$ above, where π is a prime ideal in M_β above p.

Finally, we define the $\epsilon : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ given by

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

Then, ϵ is a character such that

$$\det(\hat{\rho}_{E,p}) = \epsilon^{-1}\cdot\chi_p \tag{8}$$

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

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

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

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

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

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

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

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

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

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 $j, a/b^3 \in \mathbb{Q}$ we end up with

$$-A^4j' + 720A^2 + 9j' - 1125 = 0$$
$$(-A^2j' + 32A^2 - 3j' - 450)A = 0$$

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

$$-32A^4 + 1266A^2 - 2475 = 0 \tag{15}$$

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

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 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 $3 \nmid c$. Because $p \geq 3$ and $a^2 + 3b^6 \not\equiv 0 \mod 8$ we have that $2 \nmid c$. □

Because of Lemma 3.2 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 $\mu(\sigma)$ equal to the 3-isogeny above for $\sigma \notin G_K$.

Let d be the *degree map* (see [Que00]), 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]. We can see that $(-3, 3)$ 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. 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.

Let $\mathfrak{p}_2$ and $\mathfrak{p}_3$ 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*[1]

$$N(E) = \mathfrak{p}_2^2 \cdot \mathfrak{p}_3^8 \cdot \prod_{\mathfrak{p} \mid c} \mathfrak{p}. \tag{16}$$

Proof. Let assume that $\mathfrak{p}$ is a prime in K that does not divide $2, 3$. Then from (12) and (13) we understand that E has multiplicative reduction at $\mathfrak{p}$.

Let $\mathfrak{p}_3$ be the prime in K above 3. From Tate's algorithm we can prove that E has IV^* reduction type and because $v_{\mathfrak{p}_2}(\Delta) = 14$ we have the exponent for $\mathfrak{p}_3$.

Let $\mathfrak{p}_2$ be the prime in K above 2. Because $p \geq 3$ we have that $2 \nmid c$, Lemma 3.3. So, we have

$$(v_{\mathfrak{p}(2)}(c_4), v_{\mathfrak{p}(2)}(c_6), v_{\mathfrak{p}(2)}(\Delta)) = \begin{cases} (\geq 7, 7, 8) & \text{if } v_2(b) > 0, \\ (4, 6, 8) & \text{otherwise.} \end{cases}$$

From [Pap93, Tableau IV] we conclude that E has I_0^*, I_1^* or IV^* reduction type. Applying Tate's algorithm we can show that E has neither I_0^* nor I_1^* reduction type. □

Lemma 3.5. *The conductor of A_β is*

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

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 the system of $M_{\beta,\pi}[G_{\mathbb{Q}}]$-modules $\left\{\widehat{V}_\pi(A_\beta)\right\}$ is given by

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

as it is explained in [Che10] where $M_{\beta,\pi}$ is the completion of M_β with respect to π. In the following lines we compute the Serre invariants $N_\rho = N(\rho_{E,p})$, $k_\rho = k(\rho_{E,p})$ and $\epsilon_\rho = \epsilon(\rho_{E,p})$.

[1]For some of the computations it is more convenient to use the isomorphic to E curve

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

Proposition 3.6. *The representation $\phi_{E,p} |_{I_p}$ is finite flat for $p \neq 2, 3$.*

Proof. Let $\mathfrak{p}$ be a prime above p. By Lemma 3.4 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. Finally, K is only ramified at 3 and so $I_p \subseteq G_K$. □

Proposition 3.7. *The representation $\phi_{E,p} |_{I_\ell}$ is trivial for $\ell \neq 2, 3, p$.*

Proof. Let $\mathfrak{l}$ be a prime above ℓ. Because of Lemma 3.4 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. Finally, K is only ramified at 3 and so $I_\ell \subseteq G_K$. □

Proposition 3.8. *Suppose $p \neq 2, 3$. Then $N_\rho = 972$.*

Proof. Because we want to compute the Artin conductor of $\rho_{E,p}$, we consider only ramification at primes above $\ell \neq p$.

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 $\rho_{E,p}|_{G_K} \simeq \phi_{E,p}$ and $\phi_{E,p} |_{I_\ell}$ is trivial we have that $\rho_{E,p}$ is trivial at I_ℓ. Thus, $\rho_{E,p}$ 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 that $\hat{\phi}_{E,p}|_{I_\ell}$ factors through a finite group of order divisible only by $2, 3$. Thus, $\hat{\rho}_{E,p}|_{I_\ell}$ factors through a finite group of order divisible only by $2, 3$. It follows that the exponent of ℓ in the conductor of $\rho_{E,p}$ is the same as in the conductor of $\hat{\rho}_{E,p}$ as $p \neq 2, 3$. □

Proposition 3.9. *Suppose $p \neq 2, 3$. Then $k_\rho = 2$.*

Proof. The weight is determined by $\rho_{E,p}|_{I_p}$. For $p \neq 3$ we have that K is unramified at p and so $I_p \subset G_K$. Because $\rho_{E,p}|_{G_K} \simeq \phi_{E,p}$, $\phi_{E,p} |_{I_p}$ is finite flat and the determinant of $\phi_{E,p}$ 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 $\hat{\rho}_{E,p}$. □

From [Ell04, Proposition 3.2] and Lemma 3.3 we have

Proposition 3.11. *Let assume that $\rho_{E,p}$ 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 3.11 and Lemma 3.3 is the following.

Corollary 3.12. *The representation $\rho_{E,p}$ is irreducible for $p \neq 2, 3, 5, 7, 13$.*

Proposition 3.13. *If $p = 13$, then $\rho_{E,p}$ 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

Proof. Let assume that $p \geq 11$ be an odd prime. Let (a,b,c) be a primitive solution of (2). We attach to (a,b,c) the curve E. Because of the modularity of $\mathbb{Q}$-curves which follows from Serre's conjecture [KW09a, KW09b, Kis09], the Ribet's level lowering [Rib90] and the results in Section 3 we have that there exists a newform $f \in S_2(\Gamma_0(972))$ such that $\rho_{E,p} \simeq \rho_{f,p}$.

There are 7 newforms of level 972. Four of them are rational[2] with complex multiplication by $\mathbb{Q}(\sqrt{-3})$ and the other three 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 use Proposition 4.1 and we prove that $p \leq 7$ (see *CongruenceCriterion.m*). □

Proposition 4.1. *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*

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

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 $\rho_{A_\beta,\pi} = \rho_{E,p}$ where $\rho_{A_\beta,\pi}$ is the mod π representation of $G_\mathbb{Q}$ on the π^n-torsion points of A_β. We recall that

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

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

Let assume the case $a^2 + 3b^6 \equiv 0 \mod q$. By (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 $a^2+3b^6 \not\equiv 0 \mod q$. When $\left(\frac{-3}{q}\right) = 1$ we have that $\sigma = \mathrm{Frob}_q \in G_K$ and $\mu(\sigma) = 1$, $d(\sigma) = 1$, so $\mathrm{Tr}\,\rho_{A_\beta,\pi}(\sigma) = \mathrm{Tr}\,\phi_{E,p}(\sigma)$. Because $\rho_{A_\beta,\pi} = \rho_{E,p} \simeq \rho_{f,p}$ we conclude that $a_q(E) \equiv a_q(f) \mod \pi$ 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 $\mathrm{Tr}\,\rho_{A_\beta,\pi}(\sigma^2) = \mathrm{Tr}\,\phi_{E,p}(\sigma^2) = a_{q^2}(E)$. We know that

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

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

---

[2]Let f be a newform and K_f the eigenvalues field of f. Then we say that f is *rational* when $K_f = \mathbb{Q}$ and *irrational* when $K_f \neq \mathbb{Q}$.

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 $\mathbb{P}\rho_{E,p}$ 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 $\mathbb{P}\rho_{E,p}$ lies in the normalizer of a nonsplit 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 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 reasons why Proposition 5.3 implies Proposition 5.2 are 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 $d = 3$, $\chi_{-3} = \left(\frac{-3}{n}\right)$ and $q = 3$. 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 primitive solutions of* (2) *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 3.3 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 5.4 we have that $\rho_{E,p}$ does not lie in the normalizer of a Cartan group for $p \neq 13$. However, this is a contradiction to the fact that $\rho_{E,p} \simeq \rho_{f,p}$.

For $p = 13$ we have problem only for the split case which we can not exclude using Proposition 5.1. 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 the remaining small exponents

In this final section we finish the proof of Theorem 1 proving that (2) has no primitive solutions for $n = 3, 4, 5, 7$. We need the following lemma.

Lemma 6.1. *Let $p \geq 5$ 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. This is a consequence of factoring $x^2 + 3y^2 = z^p$ over the ring of integers of $\mathbb{Q}(\sqrt{-3})$. □

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

$$\left(\frac{a}{b^3}\right)^2 = \left(\frac{c}{b^2}\right)^3 - 3. \tag{27}$$

The curve E is Cremona's label 972B1 with trivial Mordell-Weil group [Cre97].

6.2. **Case $n = 4$:** Let assume that $n = 4$. We know that $2 \mid b$. For the parametrization of the conic $X^2 + 3Y^2 = 1$ we have that there exist coprime $x, y \in \mathbb{Z}$ such that

$$\begin{cases} \dfrac{a}{c^2} = \dfrac{3x^2 - y^2}{3x^2 + y^2} \\ \dfrac{b^3}{c^2} = \dfrac{-2xy}{3x^2 + y^2} \end{cases} \tag{28}$$

Because a,c are odd we understand that there exists $k\geq 0$ such that

$$\begin{cases} a = \dfrac{3x^2-y^2}{2^k} \\ c^2 = \dfrac{3x^2+y^2}{2^k} \\ b^3 = \dfrac{-2xy}{2^k} \end{cases} \tag{29}$$

Lemma 6.2. *Let a,b,c,x,y as above. Then $k=0$.*

Proof. Let assume that $k>0$. Because a is odd we have that x,y are odd too. Since $3x^2-y^2\equiv 2 \mod 4$ we have that $k=1$. Then $3x^2+y^2\equiv 0 \mod 4$ and so $2\mid c$ which is a contradiction. □

Because c is odd and Lemma 6.2 we have that $2\nmid y$. So, we conclude that there are coprime integers b_1,b_2 such that $x=4b_1^3$ and $y=b_2^3$. Thus we have that

$$c^2 = 48b_1^6+b_2^6 \tag{30}$$

Because $b_1\neq 0$ the point $(\frac{b_2}{b_1},\frac{c}{b_1^3})$ is a rational point on the genus 2 curve

$$C: Y^2 = X^6+48 \tag{31}$$

Unfortunately, the Jacobian of C has rank 2 and classical Chabauty method does not work. However, C is bielliptic and we are able to apply the ideas in [FW99]. In the Appendix 7 we prove the following

Proposition 6.3. *The set of rational points of C is $C(\mathbb{Q})=\{\infty^{\pm},(\pm1,\pm7)\}$.*

From $C(\mathbb{Q})$ it is easy to compute the solutions of (2) for $n=4$.

6.3. **Case $n=5$:** 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 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 we have that

$$(u^2+\sqrt{-3}v^2)^2-2^2\cdot 3^2\cdot 5^7\cdot b_1^{12} = b_2^3. \tag{32}$$

Then the point $(\frac{b_2}{5^2\cdot b_1^4},\frac{u^2+\sqrt{-3}v^2}{5^3\cdot b_1^6})$ is a $\mathbb{Q}(\sqrt{-3})$-point of the elliptic curve $E:Y^2=X^3+180$. However, using Magma we can prove that $E(\mathbb{Q}(\sqrt{-3}))$ is trivial which is a contradiction.

For the second case we have

$$5u^4-30u^2b_1^6+9b_1^{12} = W_1^2-20u^4 = b_2^3. \tag{33}$$

where $W_1=3b_1^6-5u^2$. Firstly, we consider the case $(u,b_1)\equiv(1,1) \mod 2$. Then we understand that there exists odd W_1' such that $W_1=2W_1'$. Thus, we have

$$W_1'^2-5u^2 = 2b_2'^3 \tag{34}$$

where $b_2=2b_2'$. Taking the last equation modulo 4 we understand that $2\mid b_2'$, thus $W_1'^2-5u^2\equiv 0 \mod 8$ which is a contradiction to the fact that both W_1' and u are odd.

Let assume now that one of the b_1 and u is even[3]. Then we deduce W_1 is coprime to 10. Factoring (33) over $\mathbb{Q}(\sqrt{5})$, which has class number 1, we have that there exist m and n both odd or even such that

$$W_1 + 2\sqrt{5}u^2 = \left(\frac{1+\sqrt{5}}{2}\right)^e \left(\frac{m+n\sqrt{5}}{2}\right)^3. \tag{35}$$

where $e = 0, 1, 2$.

For the case $e = 1$ and expanding (35) we have that

$$\begin{aligned} m^3 + 15m^2n + 15mn^2 + 25n^3 =& 16W_1 \\ m^3 + 3m^2n + 15mn^2 + 5n^3 =& 32u^2 \end{aligned}$$

Subtracting the last two equations we get $3m^2n + 5n^3 = 4W_1 - 8u^2$. Because m and n are both odd or even we deduce $3m^2n + 5n^3 \equiv 0 \mod 8$ while $4W_1 - 8u^2 \equiv 4 \mod 8$ which is a contradiction.

For $e = 2$ we have

$$\begin{aligned} 3m^3 + 15m^2n + 45mn^2 + 25n^3 =& 16W_1 \\ m^3 + 9m^2n + 15mn^2 + 15n^3 =& 32u^2 \end{aligned}$$

From the last two equations we have $3m^2n + 5n^3 = 24u^2 - 4W_1$. As before we have that $3m^2n + 5n^3 \equiv 0 \mod 8$ while $24u^2 - 4W_1 \equiv 4 \mod 8$ which is a contradiction.

Finally, we have the case $e = 0$. It holds

$$m(m^2 + 15n^2) = 8W_1 = 8(3b_1^6 - 5u^2) \tag{36}$$

$$n(3m^2 + 5n^2) = 16u^2 \tag{37}$$

From the last two equations we have

$$48b_1^6 = (m + 5n)(2m^2 + 5mn + 5n^2) \tag{38}$$

Because $\gcd(m, n) \mid 2$ and from (37) we have that $n = 2^{e_1}3^{e_2}n_1^2$ for some integer $n_1 \in \mathbb{Z}$ and $e_i \in \{0, 1\}$. Moreover, if we consider (37) modulo 5 we understand that $(e_1, e_2) = (1, 0)$ or $(0, 1)$. For the case, $(e_1, e_2) = (1, 0)$ we have that $n = 2n_1^2$. Because $m \equiv n \mod 2$ we have $m = 2m_1$ and equations (36) and (37) become

$$m_1(m_1^2 + 15n_1^4) = 3b_1^6 - 5u^2 \tag{39}$$

$$n_1^2(3m_1^2 + 5n_1^4) = 2u^2 \tag{40}$$

From (39) we conclude that m_1 is odd since one of b_1, u is even. As long as m_1 is odd we also understand from (39) that n_1 is even. However, from (40) we have that $2v_2(n_1) = 1 + 2v_2(u)$ which is a contradiction.

Let assume now that $(e_1, e_2) = (0, 1)$ and so $n = 3n_1^2$. From (38) we understand that $3 \mid m$ which is a contradiction to the fact that m, n are coprime away from 2.

6.4. **Case** $n = 7$**:** Finally, let assume that $n = 7$. 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 such that

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

[3] This case is the same like the second case of equation (12) in [BC12].

We define $f = 7u^6 - 105u^4v^2 + 189u^2v^4 - 27v^6$. From the theory of invariants of cubic binary forms (see [Cre99] or [Dah08]) we have that $28h^3 = g^2 + 27f^2$ where

$$h = 7u^4 - 18u^2v^2 + 27v^4 \tag{41}$$

$$g = 91u^6 - 189u^4v^2 - 567u^2v^4 + 729v^6. \tag{42}$$

Let $M = \mathbb{Q}(\sqrt{-3})$ and $\omega = \frac{1+\sqrt{-3}}{2}$. Then it holds $28h^3 = (g + 3\sqrt{-3}f)(g - 3\sqrt{-3}f)$.

Lemma 6.4. *Let $S_M = \{\mathfrak{p} \subset \mathcal{O}_M : \mathfrak{p}|2,3,7\}$. The triple (g, f, h) is S_M-primitive and there exist $z_1, z_2 \in M$ and $d_1, d_2 \in M(S_M, 3)$ with $d_1d_2/28 \in M^{*3}$ such that*

$$g + 3\sqrt{-3}f = d_1z_1^3 \tag{43}$$

$$g - 3\sqrt{-3}f = d_2z_2^3 \tag{44}$$

Proof. Because of [Bru03, Lemma 3.1] it is enough to prove that (g, f, h) is S_M-primitive. Because $g, f, h \in \mathbb{Q}$ it is enough to prove that $p \nmid \gcd(g, f, h)$ for $p \neq 2, 3, 7$.

Let assume that there exists a prime p that divides f, g and h. It holds

$$\mathrm{Res}(f, g; u) = 2^{42} \cdot 3^{18} \cdot 7^6 \cdot v^{36}$$
$$\mathrm{Res}(f, g; v) = 2^{42} \cdot 3^{18} \cdot 7^6 \cdot u^{36}$$

Because p has to divide both $\mathrm{Res}(f, g; u)$ and $\mathrm{Res}(f, g; v)$, $p \neq 2, 3, 7$ and $(u, v) = 1$ we have the result. □

Because $f = b_2^3, 7b_2^3$ and from Lemma 6.4 we have that

$$g + 3a\sqrt{-3}b_2^3 = d_1z_1^3$$
$$g - 3a\sqrt{-3}b_2^3 = d_2z_2^3$$

where $a = 1, 7$. Subtracting the above two equation we have the following

Proposition 6.5. *With the notation as above we have that (z_1, z_2, b_2) corresponds to a point on the cubic form*

$$C : 6a\sqrt{-3}X_3^3 = d1X_1^3 - d_2X_2^3. \tag{45}$$

where $a = 7, 1$ and $(X_1, X_2, X_3) \in \mathbb{P}^2(M)$.

Using Magma we can find a degree 9 birational map ϕ_C defined over M from C to the Jacobian E_C of C which is an elliptic curve defined over M. Again using Magma we prove that E_C has zero rank for any choice of d_1, d_2 and a.

Let $P = (a_1, a_2, a_3) \in \mathbb{P}^2(M)$ be point on C which lies in the preimage of $E_C(M)$ with $a_3 = 1, 0$. Then there exists $\lambda \in M$ such that $z_1 = \lambda a_1$, $z_2 = \lambda a_2$ and $b_2 = \lambda a_3$. For the case $a_3 = 0$ we conclude that $f = b_2 = 0$ which means that $b = 0$ in (2). Let assume that $a_3 = 1$, so $b_2 = \lambda$. Because $b_2, g \in \mathbb{Z}$ we have that $g = (d_1a_1^3 - 3a\sqrt{-3})b_2^3 \in \mathbb{Q}$. But using Magma we prove that this never happens and so (2) has no solutions for $n = 7$ (see *Exponent7.m*).

7. Appendix

In this section we prove Proposition 6.3 applying the ideas of Flynn and Wetherell [FW99] and the elliptic curve Chabauty [Bru03].

We recall that $C : Y^2 = X^6 + 48$. We define

$$E : y^2 = x^3 + 48 \tag{46}$$

It holds $E(\mathbb{Q}) = \mathbb{Z}$ and the generator is $(1, 7)$. Let $K = \mathbb{Q}(a)$ where $a^3 + 48 = 0$ and $\{0, (1, 7)\}$ be a set of representatives of $E(\mathbb{Q})/2E(\mathbb{Q})$. According to [FW99, Lemma 1.1(a)] the square of the X-coordinate of a rational point of C is the x-coordinate of one of the two elliptic curves,

$$E_1 : y^2 = x(x^2 + ax + a^2) \tag{47}$$

$$E_2 : y^2 = (1 - a)x(x^2 + ax + a^2) \tag{48}$$

For both curves have rank $E_i(K) < 3$, so we can apply elliptic curve Chabauty [Bru03] (see also [BT04], [FW99]) to compute $E_i(K) \cap E_i(\mathbb{Q})$. Writing a Magma script (see[4] *Exponent4.m*) we prove the following,

Proposition 7.1. *It holds,*

$$E_1(K) \cap E_1(\mathbb{Q}) = \{\infty, (0, 0)\}$$
$$E_2(K) \cap E_2(\mathbb{Q}) = \{\infty, (0, 0), (1 \pm 7)\}$$

Then we can easily prove that $C(\mathbb{Q}) = \{\infty^{\pm}, (\pm 1, \pm 7)\}$.

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

[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.

[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.

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

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

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

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

[4] In *Exponent4.m* we make the change of variables $(x, y) = (X/(1 - a), Y/(1 - a))$ for E_2 to bring the curve in the standard Weierstrass form.

[Cre99] J. E. Cremona. Reduction of Binary Cubic and Quartic Forms. *LMS Journal of Computation and Mathematics*, 2:62–92, 1999.

[Dah08] Sander R. Dahmen. *Classical and modular methods applied to Diophantine equations*. PhD thesis, Utrecht University, 2008.

[DDT97] H. Darmon, F. Diamond, and R. Taylor. *Elliptic curves, modulad forms & Fermat's Last Theorem (Hong Kong, 1993)*, chapter Fermat's Last Theorem, pages 2–140. International Press, 1997.

[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.

[FW99] E. Victor Flynn and Joseph L. Wetherell. Finding rational points on bielliptic genus 2 curves. *Manuscripta Mathematica*, 100(4):519–533, 1999.

[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.

[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 $\mathrm{Gal}(\overline{Q}/Q)$ 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 $\mathrm{Gal}(\overline{Q}/Q)$. *Duke Math. J.*, 54(1):179–230, 1987.

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

E-mail address: akoutsianas@math.ubc.ca