THE FERMAT-TYPE EQUATIONS $x^5 + y^5 = 2z^p$ OR $3z^p$ SOLVED THROUGH $\mathbb{Q}$-CURVES

LUIS DIEULEFAIT AND NUNO FREITAS

Abstract. We solve the Diophantine equations $x^5 + y^5 = dz^p$ with $d = 2, 3$ for a set of prime numbers of density $3/4$. The method consists of relating a possible solution to another Diophantine equation and solving the latter via a generalized modular technique. Indeed, we will apply a multi-Frey technique with two $\mathbb{Q}$-curves along with a new technique for eliminating newforms.

1. Introduction

Equations of the form

$$(1) \quad x^5 + y^5 = dz^p$$

were studied by Billerey in [1] and then by Billerey-Dieulefait in [2] by using the classic modular approach via elliptic curves over $\mathbb{Q}$. Their work includes the solution for infinitely many values of $d$, but the method there does not work in the cases $d = 2$ or $d = 3$. In this work we will solve equation (1) for another infinite set of values for $d$ (including $d = 2, 3$) via a generalized modular technique. Briefly, we will first use $\mathbb{Q}$-curves as Frey-curves as in the work of Ellenberg [7], Dieulefait-Jimenez [6] and Chen [4]. Then, as in the work of Bennett-Chen [5], we will apply the multi-Frey technique using two elliptic curves, but in our case with both curves being $\mathbb{Q}$-curves. To complete our strategy we also need to introduce a new technique to eliminate newforms.

We call a triple $(a, b, c) \in \mathbb{Z}^3$ such that $a^5 + b^5 = dc^p$ and $(a, b) = 1$ a primitive solution to (1), and we will say it is a trivial solution if also $|abc| \leq 1$. Let $\beta$ be an integer divisible only by primes $l \not\equiv 1 \pmod{5}$. In what follows we will show that for $d = 2\beta$ or $d = 3\beta$ there is a subset of the prime numbers with density $3/4$ such that there are no non-trivial primitive solutions to (1). More precisely, we will prove the following theorems:

**Theorem 1.1.** For any $p > 13$ such that $p \equiv 1 \pmod{4}$ or $p \equiv \pm 1 \pmod{5}$, the equation $x^5 + y^5 = 2\beta z^p$ has no non-trivial primitive solutions.

**Theorem 1.2.** For any $p > 73$ such that $p \equiv 1 \pmod{4}$ or $p \equiv \pm 1 \pmod{5}$, the equation $x^5 + y^5 = 3\beta z^p$ has no non-trivial primitive solutions.


2010 Mathematics Subject Classification. Primary 11D41.

The first author’s research was supported by project MICINN MTM2009-07024 from MECD, Spain; and ICREA Academia Research Prize.

The second author’s research was supported by a scholarship from Fundação para a Ciência e a Tecnologia, Portugal, reference no. SFRH/BD/44283/2008.

©2013 American Mathematical Society
Reverts to public domain 28 years from publication
We want to point out that in sections 5.1 and 5.2 we will first prove weaker results than the above (Theorem 5.1 and 5.2). Then by using the multi-Frey technique we finish the proofs of Theorem 1.1 and Theorem 1.2 in section 5.3.

2. A PAIR OF DIOPHANTINE EQUATIONS

From now on we will consider \(a, b\) to be coprime integers; thus we will always be talking about primitive solutions. The first observation in order to solve equation (1) is that we will use the factorization

\[
a^5 + b^5 = (a + b)(a^4 - a^3b + a^2b^2 - ab^3 + b^4)
\]

to relate a solution to (1) with a solution of another Diophantine equation. With that in mind, we let \(\phi(a, b) = a^4 - a^3b + a^2b^2 - ab^3 + b^4\) and recall some elementary results from [1]:

**Lemma 2.1.** The integers \(a + b\) and \(\phi(a, b)\) are coprime outside 5. Moreover, if 5 divides \(a + b\), then \(v_5(\phi(a, b)) = 1\).

**Proof.** Let \(l\) be a prime number dividing \(a + b\). We have \(a^2 + b^2 \equiv -2ab \pmod{l^2}\). From \(\phi(a, b) = (a^2 + b^2)^2 - ab(a^2 + b^2 + ab)\) it follows that

\[
\phi(a, b) \equiv 5a^2b^2 \pmod{l^2}.
\]

If \(l \neq 5\) we have \(5a^2b^2 \equiv 0 \pmod{l}\) because \(l \nmid ab\), and by congruence (3) we conclude that \(l\) does not divide \(\phi(a, b)\). If \(l = 5\), then congruence (3) implies that \(l \nmid \phi(a, b)\) and \(v_5(\phi(a, b)) = 1\).

**Lemma 2.2.** Let \(l \equiv 1 \pmod{5}\) be a prime number dividing \(a^5 + b^5\). Then, \(l\) divides \(a + b\).

**Proof.** Since \(l \mid a^5 + b^5\) and \((a, b) = 1\), then \(l \nmid ab\). Let \(b'\) be the inverse of \(-b \pmod{l}\). Since \(a^5 \equiv (-b)^5 \pmod{l}\), we have \((ab')^5 \equiv 1 \pmod{l}\). Hence \(ab'\) has order 1 or 5. If \(ab'\) has order 1, then \(a + b \equiv 0 \pmod{5}\). Hence if \(l \nmid a + b\), then \(ab'\) must have order 5; thus \(5 \mid l - 1\), i.e., \(l \equiv 1 \pmod{5}\).

**Corollary 2.3.** Suppose \((a, b) = 1\). If a prime number \(q \neq 5\) divides \(\phi(a, b)\), then \(q \equiv 1 \pmod{5}\). Also, if \(5 \nmid a + b\), then \(v_5(\phi(a, b)) = 0\).

**Proof.** Let \(q \neq 5\) be a prime dividing \(\phi(a, b)\). Then \(q \mid a^5 + b^5\) by (2) and \(q \nmid a + b\) by Lemma 2.1. Hence by Lemma 2.2 we must have \(q \equiv 1 \pmod{5}\). Since \(5 \neq 1 \pmod{5}\), if \(5 \nmid a + b\) it follows from Lemma 2.2 that \(5 \nmid a^5 + b^5\); thus \(5 \nmid \phi(a, b)\).

The following lemma follows directly from Lemma 2.2 Corollary 2.3 and the equalities \(x^5 + y^5 = (x + y)^5 \phi(x, y) = d\zeta^p\).

**Lemma 2.4.** If there exists a non-trivial primitive solution \((a, b, c')\) to \(x^5 + y^5 = d\zeta^p\) with \(d \neq 0\) an integer divisible only by primes \(\neq 1 \pmod{5}\), then there exists a solution \((a, b, c)\) such that \((a, b) = 1\) and \(|abc| > 1\) to

\[
\phi(a, b) = c^p
\]

or

\[
\phi(a, b) = 5c^p,
\]

which satisfies \(5 \nmid a + b\) in case (4) and \(5 \mid a + b\) in case (5). Moreover:

- if \(m \mid d\), then \(m \mid a + b\);
• the prime divisors of $c$ are all congruent to 1 (mod 5). In particular, neither 2 nor 5 divide $c$.

From the lemma above we see that Theorems 1.1 and 1.2 will follow if we prove that there are no solutions $(a, b, c)$ to (4) and (5) such that $(a, b) = 1$ (primitive), $|abc| > 1$ (non-trivial) and $d | a + b$. We want to remark that despite $d = 2\beta$ or $d = 3\beta$ in the statements of the theorems, in their proofs we will only need $2 | d$ or $3 | d$, because this already implies that $2 | a + b$ or $3 | a + b$, which is enough to prove Theorem 1.1 or Theorem 1.2, respectively.

3. THE $Q$-CURVE

To apply the modular approach we need to find an appropriate Frey $Q$-curve. Consider the polynomial
\[
\phi(x, y) = x^4 - x^3 y + x^2 y^2 - xy^3 + y^4
\]
and its factorization over $\mathbb{Q}(\sqrt{5})$,
\[
\phi(x, y) = \phi_1(x, y)\phi_2(x, y),
\]
where
\[
\begin{align*}
\phi_1(x, y) & = x^2 + \omega xy + y^2, \\
\phi_2(x, y) & = x^2 + \bar{\omega} xy + y^2, \\
\omega & = \frac{-1 + \sqrt{5}}{2}, \\
\bar{\omega} & = \frac{-1 - \sqrt{5}}{2}.
\end{align*}
\]

**Proposition 3.1.** If $(a, b)$ is a pair of coprime integers, then $\phi_1(a, b)$ and $\phi_2(a, b)$ are coprime outside 5.

**Proof.** Suppose that $l$ is a prime in $\mathbb{Q}(\sqrt{5})$ dividing both $\phi_1(a, b)$; then $l$ also divides $\phi_1 - \phi_2 = \sqrt{5}ab$. If $l$ divides $ab$, then we can suppose that $l$ divides $a$, but dividing $a$ and $\phi_1(a, b)$ implies that it divides $b$ which is a contradiction since $a, b$ are coprime. Thus we conclude that $l$ is above 5. \(\square\)

Let $(a, b, c)$ be a non-trivial primitive solution to (4) or (5); we define an elliptic curve over $\mathbb{Q}(\sqrt{5})$,
\[
E_{(a, b)} : y^2 = x^3 + 2(a + b)x^2 - \bar{\omega}\phi_1(a, b)x.
\]
To ease notation we will omit the pair $(a, b)$ when writing $E_{(a, b)}$, $\phi(a, b)$, $\phi_1(a, b)$, $\phi_2(a, b)$. Observing that $(a + b)^2 = -\bar{\omega}\phi_1 - \omega\phi_2$ we compute
\[
\Delta(E) = 2^6\bar{\omega}\phi_1.
\]
Consider the Galois conjugated curve for the non-trivial element in $\text{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$,
\[
\sigma E : y^2 = x^3 + 2(a + b)x^2 - \omega\phi_2x,
\]
and the 2-isogeny $\mu : \sigma E \rightarrow E$ given by
\[
(x, y) \mapsto \left( -\frac{y^2}{2x^2}, \frac{\sqrt{-2}}{4} \frac{y}{x^2} (\omega\phi_2 + x^2) \right).
\]
with dual isogeny \( \hat{\mu} : E \to \sigma E \) given by
\[
(x, y) \mapsto (-\frac{y^2}{2x^2}, -\frac{\sqrt{-2}}{4} y \omega \phi_1 + x^2)),
\]
showing that \( E \) is a \( \mathbb{Q} \)-curve. In order to apply the modular approach to our equation, we need to find a twist of \( E \), \( E_\gamma \) such that its Weil restriction decomposes as a product of abelian varieties of \( GL_2 \)-type. That is the content of the following theorem, whose proof we postpone until section 6.

**Theorem 3.2.** Let \( K = \mathbb{Q}(\theta) \) where \( \theta = \sqrt[5]{2} (5 + \sqrt{5}) \) is a root of the polynomial \( x^4 - 5x^2 + 5 \), and put \( \gamma = 2\theta^2 - \theta - 5 \). Then, the twisted curve
\[
E_\gamma : y^2 = x^3 + 2\gamma(a + b)x^2 - \gamma^2 \omega \phi_1(a, b)x
\]
is completely defined over \( K \) and its Weil restriction decomposes as the product of two non-isogenous abelian varieties of \( GL_2 \)-type, each of them with an endomorphism algebra over \( \mathbb{Q} \) isomorphic to \( \mathbb{Q}(i) \).

3.1. The conductor of \( E_\gamma \). Now we will determine the conductor of \( E_\gamma \). These conductors are needed to compute the conductor of the Weil restriction of \( E_\gamma \) and consequently the level of the associated modular forms. Let \( K = \mathbb{Q}(\theta) \) and denote by \( \mathfrak{P}_2 \) and \( \mathfrak{P}_5 \) the only primes above 2 and 5, respectively. Also, denote the conductor of \( E_\gamma \) by \( N_{E_\gamma} \) and let \( \text{rad}(c) \) be the product of the prime factors of \( c \). The curves \( E_\gamma(a, b) \) have associated the following quantities:
\[
\Delta(E_\gamma) = \gamma^6 \Delta(E) = \gamma^6 2^6 \omega \phi_1, \\
c_4(E_\gamma) = \gamma^2 \Delta(E) = -\gamma^2 2^4 (\omega \phi_1 - 2^2 \phi_2), \\
c_6(E_\gamma) = \gamma^3 \Delta(E) = -\gamma^3 2^6 (a + b)(\omega \phi_1 - 2^3 \phi_2).
\]
Recall that \( \phi = \phi_1 \phi_2 \) over \( \mathbb{Q}(\sqrt{5}) \). If \( \phi(a, b) = c^p \) or \( \phi(a, b) = 5c^p \), then \( \phi_1(a, b) = c_i^p \) or \( \phi_i(a, b) = \sqrt{5}c_i^p \) up to units, with \( c_i \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})} \). In the following proofs we follow the tables of Papadopoulos in [9].

**Proposition 3.3.** Let \( \mathfrak{P} \) be a prime in \( K \) distinct from \( \mathfrak{P}_2 \), \( \mathfrak{P}_5 \). Then \( E_\gamma \) has good (\( v_{\mathfrak{P}}(N_{E_\gamma}) = 0 \)) or multiplicative (\( v_{\mathfrak{P}}(N_{E_\gamma}) = 1 \)) reduction if \( \mathfrak{P} \nmid c \) or \( \mathfrak{P} | c \), respectively.

**Proof.** Observe that \( \omega \) and \( \bar{\omega} \) are units. Then \( v_{\mathfrak{P}}(\Delta) = pv_{\mathfrak{P}}(c) + pv_{\mathfrak{P}}(c_1) \). Hence, if \( \mathfrak{P} \nmid c \) we have \( v_{\mathfrak{P}}(\Delta) = 0 \) and the curve has good reduction. If \( \mathfrak{P} | c \) we have \( v_{\mathfrak{P}}(\Delta) > 0 \) and since \( \mathfrak{P} \) divides only one of the \( c_i \), it is clear from the form of \( c_4(E) \) that \( v_{\mathfrak{P}}(c_4) = 0 \); thus the curve has multiplicative reduction. \( \square \)

**Proposition 3.4.** Let \( \mathfrak{P} = \mathfrak{P}_5 \). The curve \( E_\gamma \) has bad additive reduction (\( v_{\mathfrak{P}}(N) = 2 \)) or good reduction if \( 5 \nmid a + b \) or \( 5 | a + b \), respectively.

**Proof.** Note that \( \gamma \mathcal{O}_K = \mathfrak{P}_5 \). If \( 5 \nmid a + b \) we have \( v_{\mathfrak{P}}(\Delta) = v_{\mathfrak{P}}(\gamma^6 2^6 \omega c^p c_1^p) = 6 \) and \( v_{\mathfrak{P}}(c_4) > 0 \). Then by Table I in [9] the curve has bad additive reduction and \( v_{\mathfrak{P}}(N) = 2 \).

In \( 5 | a + b \) we have
\[
v_{\mathfrak{P}}(\Delta) = v_{\mathfrak{P}}(\gamma^6 2^6 5\sqrt{5} c^p c_1^p) = v_{\mathfrak{P}}(\gamma^6) + v_{\mathfrak{P}}(5) + v_{\mathfrak{P}}(\sqrt{5}) = 6 + 4 + 2 = 12.
\]
This means that the equation is not minimal. Any change of variable leading to a minimal equation will decrease the valuation of the discriminant by 12, hence \( v_\pi(\Delta) = 0 \), i.e. the curve as good reduction.

Let \( \pi = \mathfrak{P}_2 \) and we note that \( v_\pi(2) = 2 \).

**Proposition 3.5.** The conductor at \( \pi \) of \( E_\gamma \) satisfies:

\[
v_\pi(N_{E_\gamma}) = \begin{cases} 
8 \text{ or } 6 & \text{if } 2 \nmid a + b, \\
8 & \text{if } 2 \mid a + b, \\
0 & \text{if } 4 \mid a + b, \\
4 & \text{if } 8 \mid a + b.
\end{cases}
\]

**Proof.** Observe that \((v_\pi(c_4), v_\pi(c_6), v_\pi(\Delta)) = (8, 12 + 2v_2(a + b), 12)\). According to Table V in [9] these values can correspond to the Tate cases 3, 6, 7 \((\nu \text{ odd})\), 7 \((\nu \text{ even}), 9, 10 \text{ or non-minimal}\). The fact \( v_\pi(\Delta) = 12 \) tells us that if we arrive at the non-minimal case then the curve has good reduction; hence we go through each case only once. Observe from Proposition 6 in [9] that \( \pi^{10} \) is the highest power of \( \pi \) appearing in the congruences used to decide which case we are in for each \((a, b)\). Since between our possible cases the coordinate changes are translations, it follows that all the possible values for the conductor at \( \pi \) must appear by considering the pairs \((a, b)\) \((\text{mod } 2^5)\). Using SAGE we compute these conductors and easily observe that they divide into categories according to the statement.

Let \( E_{\gamma,2} \) be the twist of \( E_\gamma \) by 2 and denote its conductor by \( N_{E_{\gamma,2}} \). This conductor will later be used to reach a contradiction when analyzing representations coming from newforms. Actually, we will only need it in the case of congruences between representations coming from newforms with level 1600 and \( E_\gamma(a, b) \), where \( 2 \parallel a+b \).

**Proposition 3.6.** Suppose that \((a, b, c)\) is a solution to (4) or (5) such that \( 2 \parallel a+b \). Then the conductor at \( \pi \) of \( E_{\gamma,2} \) is \( \pi^0 \) or \( \pi^4 \).

**Proof.** Observe that when twisting a curve by 2 the quantities \( \Delta, c_4 \) and \( c_6 \) change by the factors \( 2^6, 2^2 \) and \( 2^3 \), respectively. Then for \( E_{\gamma,2} \) we have \((v_\pi(c_4), v_\pi(c_6), v_\pi(\Delta)) = (12, 18+2v_2(a+b), 24)\) and by Table V in [9] it follows that the equation is not minimal. After the change \((x, y) = (\pi^2x, \pi^3y)\) we have \((v_\pi(c_4), v_\pi(c_6), v_\pi(\Delta)) = (8, 12 + 2v_2(a+b), 12)\). Now exactly as above but with the extra condition \( 2 \parallel a+b \) we use SAGE to compute the conductors.

4. **Modularity of \( E_\gamma \)**

Here we determine the precise Serre parameters: weight, level and character of a residual representation of a \( GL_2 \)-type abelian variety attached to our Frey-curves.

Let \( B = \text{Res}_{K/Q}(E_\gamma/K) \), where \( K = Q(\theta) \) is the cyclic Galois extension as before, and denote its conductor by \( N_B \). To compute this conductor we will use a formula of Milne (see [3]), which in our case tells us that the conductor satisfies

\[
N_B = \text{Nm}_{K/Q}(N_{E_\gamma})\text{Disc}(K/Q)^2,
\]

where \( \text{Disc} \) and \( \text{Nm} \) denote the discriminant and norm of \( K/Q \), respectively. Since \( c \) is odd and \( \text{Disc}(K/Q) = 2^45^3 \), then the primes dividing \( c \) do not ramify in \( K \).
Being $K/\mathbb{Q}$ of degree 4 we have that a prime $p$ dividing $c$ is inert, splits completely or is the product of two primes in $K$ with residual degree 2; thus $\text{Nm}((c)) = c^4$. Also, $\text{Nm}((\mathcal{P}_5)) = 5$ and $\text{Nm}((\mathcal{P}_2)) = 4$. By applying the above formula we obtain the following results:

**Proposition 4.1.** If $(a, b, c)$ is a primitive solution of equation (4), then $B$ has conductor:

$$N_B = \begin{cases} 
2^{245^8} \text{rad}(c)^4 \text{ or } 2^{20^5} \text{rad}(c)^4 & \text{if } 2 \mid a + b, \\
2^{245^8} \text{rad}(c)^4 & \text{if } 2 \parallel a + b, \\
2^{5^8} \text{rad}(c)^4 & \text{if } 4 \parallel a + b, \\
2^{16^5} \text{rad}(c)^4 & \text{if } 8 \mid a + b. 
\end{cases}$$

**Proposition 4.2.** If $(a, b, c)$ is a primitive solution of equation (5), then $B$ has conductor:

$$N_B = \begin{cases} 
2^{245^8} \text{rad}(c)^4 \text{ or } 2^{20^5} \text{rad}(c)^4 & \text{if } 2 \mid a + b, \\
2^{245^8} \text{rad}(c)^4 & \text{if } 2 \parallel a + b, \\
2^{5^8} \text{rad}(c)^4 & \text{if } 4 \parallel a + b, \\
2^{16^5} \text{rad}(c)^4 & \text{if } 8 \mid a + b. 
\end{cases}$$

We know from Theorem 3.2 that $B \simeq S_1 \times S_2$, where $S_i$ are two non-$\mathbb{Q}$-isogenous abelian surfaces of $GL_2$-type with $\mathbb{Q}$-endomorphism algebras equal to $\mathbb{Q}(i)$. So the conductor of $B$ satisfies $N_B = N_{S_1}N_{S_2}$.

For a prime $l$ and each $S_i$ the action on the Tate module $T_iS_i$ induces a 4-dimensional $l$-adic representation of $G_\mathbb{Q}$ that decomposes into two 2-dimensional $\lambda$-adic representations $\rho_{S_i, \lambda}$ and $\rho_{S_i, \lambda}^\sigma$, where $\lambda$ is a prime of $\mathbb{Q}(i)$ above $l$. Then we have four 2-dimensional representations of $G_\mathbb{Q}$ extending the $l$-adic representation $\rho_{E_{\gamma},l}$ of $\text{Gal}(\overline{\mathbb{Q}}/K)$ induced by the action on the Tate module of $E_{\gamma}$. Since extensions of absolutely irreducible representations are unique up to twists, we have the following relations between them:

$$\begin{cases} 
\rho_{S_1, \lambda} \otimes \epsilon \sim \rho_{S_1, \lambda}^\sigma, \\
\rho_{S_1, \lambda} \otimes \epsilon^2 \sim \rho_{S_2, \lambda}, \\
\rho_{S_1, \lambda} \otimes \epsilon^3 \sim \rho_{S_2, \lambda}^\sigma,
\end{cases}$$

where $\epsilon$ is the character of $K$ (see section 6 formula (19)) and $\epsilon^2$ is the character of $\mathbb{Q}(\sqrt{5})$. It is known that the conductors of $\rho_{S_1, \lambda}$ and $\rho_{S_1, \lambda}^\sigma$ are equal and that their product is equal to the conductor of $S_1$, which means that every prime in the conductor of $S_1$ appears to an even power. From the second of the three relations above and the fact that $\epsilon^2$ has conductor 5, we see that the only possible difference in the conductors of $\rho_{S_1, \lambda}$ and $\rho_{S_2, \lambda}$ may occur at 5. Furthermore, the conductor at 5 of $\rho_{S_1, \lambda} \otimes \epsilon^2$ is smaller than or equal to the least common multiple between the conductor at 5 of $\rho_{S_1, \lambda}$ and $\text{cond}_5(\epsilon^2)^2$; that is,

$$\text{cond}_5(\rho_{S_1, \lambda} \otimes \epsilon^2) \leq \text{lcm}(\text{cond}_5(\rho_{S_1, \lambda}), \text{cond}_5(\epsilon^2)^2) = \text{lcm}(\text{cond}_5(\rho_{S_1, \lambda}), 5^2).$$

The inequality may hold only if the conductor at 5 of $\rho_{S_1, \lambda}$ is equal to $5^2$. Using these facts together with a case checking allows us to determine all the possibilities for the conductors of the four 2-dimensional representations $\rho_{S_1, \lambda}$, $\rho_{S_1, \lambda}^\sigma$ where $i = 1$ or 2 (see Table 1).
Table 1. Values of conductors, where \( c_0 = \text{rad}(c) \)

<table>
<thead>
<tr>
<th>Equation</th>
<th>( v_2(a + b) )</th>
<th>( \rho S_1,\lambda )</th>
<th>( \rho^2 S_1,\lambda )</th>
<th>( \rho S_2,\lambda )</th>
<th>( \rho^2 S_2,\lambda )</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>0</td>
<td>( 2^65^2c_0 )</td>
<td>( 2^65^2c_0 )</td>
<td>( 2^65^2c_0 )</td>
<td>( 2^65^2c_0 )</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>( 2^55^2c_0 )</td>
<td>( 2^55^2c_0 )</td>
<td>( 2^55^2c_0 )</td>
<td>( 2^55^2c_0 )</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>( 2^65^2c_0 )</td>
<td>( 2^65^2c_0 )</td>
<td>( 2^65^2c_0 )</td>
<td>( 2^65^2c_0 )</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>( 2^25^2c_0 )</td>
<td>( 2^25^2c_0 )</td>
<td>( 2^25^2c_0 )</td>
<td>( 2^25^2c_0 )</td>
</tr>
<tr>
<td>4</td>
<td>( \geq 3 )</td>
<td>( 2^45^2c_0 )</td>
<td>( 2^45^2c_0 )</td>
<td>( 2^45^2c_0 )</td>
<td>( 2^45^2c_0 )</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>( 2^65^2c_0 )</td>
<td>( 2^65^2c_0 )</td>
<td>( 2^65c_0 )</td>
<td>( 2^65c_0 )</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>( 2^65^2c_0 )</td>
<td>( 2^65^2c_0 )</td>
<td>( 2^55c_0 )</td>
<td>( 2^55c_0 )</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>( 2^25^2c_0 )</td>
<td>( 2^25^2c_0 )</td>
<td>( 2^25c_0 )</td>
<td>( 2^25c_0 )</td>
</tr>
<tr>
<td>5</td>
<td>( \geq 3 )</td>
<td>( 2^45^2c_0 )</td>
<td>( 2^45^2c_0 )</td>
<td>( 2^45c_0 )</td>
<td>( 2^45c_0 )</td>
</tr>
</tbody>
</table>

Now pick a prime \( \lambda \) in \( \mathbb{Q}(i) \) above \( p \) and let \( \rho := \rho S_1,\lambda \) and \( \bar{\rho} := \bar{\rho} S_1,\lambda \) be its residual representations. Recall that the Frey-Hellegouarch argument (used in the proof of FLT) states that a prime of semistable reduction of an elliptic curve \( C \) which appears in the discriminant of \( C \) to a \( p \)-power will not ramify in the mod \( p \) representation induced by the \( p \)-torsion points. From formula (6), Proposition 3.1 and the fact that the primes in \( K \) dividing \( c \) are of semistable reduction for \( \bar{\rho} \), we can apply the Frey-Hellegouarch argument to conclude that the restriction \( \bar{\rho}|_{\text{Gal}(\mathbb{Q}/K)} \) of \( \bar{\rho} \) to \( \text{Gal}(\mathbb{Q}/K) \), which coincides with \( \bar{\rho}_{E[p]} \), will not ramify at primes dividing \( c \). Since \( K \) only ramifies at 2 and 5, we see that \( \bar{\rho} \) cannot ramify outside 2 and 5.

On the other hand it is well known that in the presence of wild ramification the conductor does not decrease when reducing mod \( p \), so the possible conductors of \( \bar{\rho} \) are exactly the values in the third column of Table 1 without the factor \( c_0 \). Hence we have determined Serre’s level \( N(\bar{\rho}) \) needed to apply Serre’s strong conjecture (which is now a theorem). The following two propositions tell us the Serre weight and character.

**Proposition 4.3.** The representation \( \bar{\rho} \) has character \( \bar{\epsilon} \) (conjugate of \( \epsilon \)).

**Proof.** By Theorem 5.12 of [10] we know that the character associated to \( \rho S_1,\lambda \) is equal to \( \epsilon^{-1} \), where \( \epsilon \) is the splitting character defined by formula (9) in section 6. Furthermore, since \( \epsilon \) has order 4, for any prime \( p \) distinct from 2 the representation \( \bar{\rho} \) has the same character as the non-residual one. Then \( \bar{\rho} \) is modular with character \( \epsilon^{-1} = \bar{\epsilon} \).

**Proposition 4.4.** The Serre weight of the representation \( \bar{\rho} \) is \( k(\bar{\rho}) = 2 \).

**Proof.** We divide in two cases. If \( p \nmid c \), then \( S_1 \) has good reduction at \( p \) and \( \bar{\rho} \) comes from an abelian variety with good reduction at \( p \); hence \( k = 2 \). If \( p \mid c \), the fact that \( p \mid v_p(\Delta) \) for any \( \Delta \) above \( p \) implies as in [7] that \( \bar{\rho} \) is finite, so \( k = 2 \).

Finally, to apply the Serre’s conjecture we still need irreducibility.

**Proposition 4.5.** The representation \( \bar{\rho} \) is absolutely irreducible.
Proof. If \((a, b, c)\) is a non-trivial solution, then there is a prime of characteristic greater than 3 of semistable reduction. Hence by Proposition 3.2 in \([7]\) we conclude that \(\bar{\rho}\) is irreducible for \(p > 13\). \(\square\)

Now from Serre’s strong conjecture we know that there must be a newform \(f\) in the space \(\mathcal{S}_2(M, \bar{\epsilon})\) with \(M = 1600, 800, 400\) or \(100\) and \(\wp \mid p\) in \(\mathbb{Q}_f\) such that the mod \(\wp\) residual representation attached to \(f\) (denoted by \(\bar{\rho}_{f, \wp}\)) is isomorphic to our residual representation \(\bar{\rho}\).

5. Eliminating newforms

Using software we will compute the newforms in the spaces \(\mathcal{S}_2(M, \bar{\epsilon})\) with \(M = 1600, 800, 400\) or \(100\), determined in the previous section. Then, in order to reach a contradiction, we need to show that our representation \(\bar{\rho}\) cannot be isomorphic to a representation of the form \(\bar{\rho}_{f, \wp}\), where \(f\) is one of the computed newforms.

Note that equations \(\phi(a, b) = \pm 1\) and \(\phi(a, b) = \pm 5\) have solutions \((\pm 1, 0), (0, \pm 1), (1, 1), (-1, -1), (1, -1), (-1, 1)\), respectively. This means that for these pairs \((a, b)\) the Frey \(\mathbb{Q}\)-curves do exist, and so if their corresponding newforms have level \(100, 400, 800\) or \(1600\) a priori we may not be able to eliminate those forms. From now on, when we say ‘eliminate a newform’ we mean that we show that the isomorphism \(\bar{\rho} \sim \bar{\rho}_{f, \wp}\) cannot hold for any prime \(\wp \mid p\). Recall that when treating the case \(2 \mid d\) or \(3 \mid d\) we have \(a + b\) even or \(3 \mid a + b\), respectively. As we will see this will turn out to be key information. Now observe that \((\pm 1, 0), (0, \pm 1)\) will not be a problem for equation \((\mathbf{4})\) when \(2 \mid d\), because \(a + b\) is odd;

Since the elliptic curves \(E(1, -1), E(1, 1), E(1, -1)\) and \(E(1, 1)\) correspond to newforms with complex multiplication, we will also be able to eliminate them.

To eliminate the newforms we will separate them into three sets and then we apply a different strategy for each of the sets. Given a newform \(f\) let \(\mathbb{Q}_f = \mathbb{Q}(\{a_q(f)\})\) be its field of coefficients and note that for those we will compute we have \(\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-5}) \subseteq \mathbb{Q}_f\). Now let \(S_1, S_2\) and \(S_3\) be as follows:

- \(S_1\): Newforms with CM (Complex Multiplication),
- \(S_2\): Newforms without CM and field of coefficients strictly containing \(\mathbb{Q}(i)\),
- \(S_3\): Newforms without CM and field of coefficients \(\mathbb{Q}(i)\).

In the following two sections we will find a contradiction for each set above, first in the case \(2 \mid d\) and second for \(3 \mid d\), which will give us the partial results in Theorem \(5.1\) and Theorem \(5.2\). We want to remark that up to this point everything will be done using only the Frey-curves \(E_{(a, b)}\).

Finally, we will introduce a new Frey \(\mathbb{Q}\)-curve \(F\) (see equation \(\mathbf{5}\)) and, from the fact that the pairs \(E(1, -1), F(1, -1), E(1, 1)\) and \(F(1, -1)\) have CM by a different field, together with the multi-Frey technique, we will finish the proof of Theorem \(1.3\) and Theorem \(1.2\).

5.1. The case \(2 \mid d\). Since \(2 \mid a + b\), then \(800 = 2^5 5^2\) is not a possible level. We compute the spaces \(\mathcal{S}_2(M, \bar{\epsilon})\) with \(M = 1600, 400\) and \(100\) and divide the newforms into the sets \(S_1, S_2\) and \(S_3\) defined above.

Newforms in \(S_1\): Modulo Galois conjugation there are 8 newforms with complex multiplication, half of them with CM by \(\mathbb{Q}(i)\) and the other half by \(\mathbb{Q}(\sqrt{-5})\). If there is a non-trivial solution \((a, b, c)\) to equation \((\mathbf{1})\) or \((\mathbf{5})\), then there exists a prime not dividing \(6\) of semistable reduction for \(E\). Hence if \(p > 13\) by Proposition
3.4 in [7], the images of \( \bar{\rho} \) will not lie in the normalizer of a split Cartan subgroup. Then if \( p \) splits in both \( \mathbb{Q}(i) \) and \( \mathbb{Q}(\sqrt{-5}) \), i.e. \( p \equiv 1 \mod 4 \) and \( p \equiv \pm 1 \mod 5 \), we can not have \( \bar{\rho} \sim \bar{\rho}_{f,p} \) for \( f \) in \( S_1 \). This is because for a newform with CM it is known that for \( p \)'s that are split on the field of complex multiplication, the image of the attached representation will be in a normalizer of a split Cartan subgroup.

**Newforms in \( S_2 \):** There are 12 newforms (modulo conjugation) in this group. For each prime \( q \) of good reduction for \( S_1 \) there is the quantity

\[
a_q(S_1) := \text{Trace}(\rho_{S_1,\lambda}(\text{Frob}_q)),
\]

and we know that it satisfies \( a_q(S_1) = \bar{a}_q(S_1)\bar{\epsilon}(q) \) from propositions 4.3 and 3.4 in [13]. In the previous equality \( \epsilon \) is the character of order 4 defined in section 6 in particular, the inner twist implies that

\[
a_q(S_1) = \begin{cases} 
t & \text{if } q \equiv 1 \text{ or } 19 \mod 20, 

t & \text{if } q \equiv 9 \text{ or } 11 \mod 20, 
\end{cases}
\]

\[
\begin{cases} 
t - \bar{t} & \text{if } q \equiv 3 \text{ or } 17 \mod 20, 
\end{cases}
\]

where \( t \) is an integer. Recall from Table I that a prime \( q \neq 2, 5 \) of bad reduction for \( S_1 \) must divide \( c \); that is, it must divide \( \phi(a, b) \). Since \( 3 \equiv 1 \mod 5 \) it follows from Corollary [22] that 3 is a prime of good reduction for \( S_1 \). Hence, \( a_q(S_1) \) must be of the form \( t - ti \), and from the Weil bound \( |a_3(S_1)| \leq 2\sqrt{3} \) it follows that \( |t| \leq 2 \). If \( f = q + \sum_{n \geq 2} c_n q^n \) is one of these 12 newforms in \( S_2 \), then the congruence

\[
a_3(S_1) \equiv c_3(f) \pmod{\mathfrak{P}}
\]

for a prime \( \mathfrak{P} \) in \( \mathbb{Q} \) above \( p \) must hold. Now for each newform in \( S_2 \) we use the coefficient \( c_3(f) \) to derive a contradiction, because none of them has \( c_3(f) \) of the form \( t - ti \). As an example, there is a newform \( f \) in \( S_2 \) of level 400 with \( c_3(f) \) having minimal polynomial \( x^2 + 10i \); thus if the congruence \( \bar{\epsilon}(7) \) holds we must have \( c_3(f) \equiv t - i \pmod{\mathfrak{P}} \) with \( t = 0, \pm 1, \pm 2 \). Taking fourth powers we get \( 100 \equiv 4t^4 \pmod{\mathfrak{P}} \), which means \( 25 - t^4 \equiv 0 \pmod{\mathfrak{P}} \), and finally, substituting for the possible values of \( t \) we reach a contradiction if \( p > 5 \). A similar argument works for every newform in \( S_2 \), and we conclude that if \( p > 7 \) the newform predicted by Serre’s conjecture cannot be in \( S_2 \).

**Newforms in \( S_3 \):** There are 10 newforms in this group, all with level 1600. Recall that \( \bar{\rho} := \bar{\rho}_{S_1,\lambda} \) and suppose that \( \bar{\rho} \sim \bar{\rho}_{f,p} \) for some \( f \) in \( S_3 \). A priori all newforms in \( S_3 \) are inconvenient in the sense that their Fourier coefficients \( a_q(f) \) behave exactly as those of our surface \( S_1 \). That is, each \( a_q(f) \) lies in \( \mathbb{Q}(i) \), they respect the rule \( a_q(f) = \bar{a}_q(f)\bar{\epsilon}(p) \) (by construction) and they are even (this is true for our surface because \( E_3 \) has a 2-torsion point). To deal with this problem we will twist each newform in \( S_3 \) by the character of \( \mathbb{Q}(\sqrt{2}) \), which we denote by \( \chi \). Note that \( \text{cond}(\chi)^2 = 8^2 = 2^6 \) and the power of 2 in 1600 is also \( 2^6 \), so as mentioned before we are in a situation where the power of 2 in the level of the twist can decrease. Indeed, using SAGE, we pick \( f \) in \( S_3 \), we consider \( f \otimes \chi \) and compare the coefficients of \( f \otimes \chi \) up to the Sturm bound with those of the newforms with level dividing 1600 to find that \( f \otimes \chi \) is a newform of level 800 for all \( f \) in \( S_3 \).

On the other hand, let \( E_{7,2} \) be as in section 3.4 and \( \rho_{E_7,2,p} \) be the representation coming from the action of \( G_{\mathbb{Q}} \) on the Tate module \( T_p E_{7,2} \). Note that

\[
(\rho_{S_1,\lambda} \otimes \chi)|K = (\rho_{S_1,\lambda})|K \otimes \chi|K = \rho_{E_7,2,p} \otimes \chi|K.
\]
that is, $\rho_{S_1, \lambda} \otimes \chi$ extends $\rho_{E_{\gamma}, p} \otimes \chi|_K$, and this one is precisely $\rho_{E_{\gamma}, 2, p}$. The same is true for the other three representations coming from the Weil restriction $B \simeq S_1 \times S_2$. Moreover, $\rho_{B, p} = \text{Ind}^G_K \rho_{E_{\gamma}, p}$ and we have

$$\rho_{B, p} \otimes \chi = (\text{Ind}^G_K \rho_{E_{\gamma}, p}) \otimes \chi = \text{Ind}^G_K (\rho_{E_{\gamma}, p} \otimes \chi|_K) = \text{Ind}^G_K \rho_{E_{\gamma}, 2, p},$$

and this means that $\rho_{B, p} \otimes \chi$ is the representation coming from the action of $G_{\mathbb{Q}}$ on the Tate module of $\text{Res}_{K/\mathbb{Q}}(E_{\gamma, 2}/K)$. Let $\rho_1$ denote the 2-dimensional factor $\rho_{S_1, \lambda} \otimes \chi$ of $\rho_{B, p} \otimes \chi$. From Proposition 5.6 Milne’s formula and an analysis identical to that used to compute Table 1 we conclude that $N(\rho_1) = 400$ or 100. $\rho_1$ is also irreducible and has character and Serre’s weight equal to those of $\bar{\rho}$, because the same arguments hold. We now apply Serre’s strong conjecture to $\bar{\rho}_1$ and we conclude that there must be a newform $g$ in level 400 or 100 and a prime $\mathfrak{p}'$ above $p$ such that $\bar{\rho}_1 \sim \bar{\rho}_g, \mathfrak{p}'$. But at the same time we also have

$$\bar{\rho}_1 = \rho_{S_1, \lambda} \otimes \chi \sim \bar{\rho} \otimes \chi \sim \bar{\rho}_f, \mathfrak{p} \otimes \chi \sim \bar{\rho}_{f \otimes \chi, \mathfrak{p}} \sim \bar{\rho}_t, \mathfrak{p},$$

where $f'$ is of level 800 by the previous paragraph. Hence the isomorphism

$$\bar{\rho}_g, \mathfrak{p}' \sim \bar{\rho}_t, \mathfrak{p}$$

must hold between a newform of level 800 and another of level 400 or 100, but Carayol has shown (see [3]) that this kind of level lowering cannot happen. At this point we have proved

**Theorem 5.1.** For any $p > 13$ such that $p \equiv 1 \mod 4$ and $p \equiv \pm 1 \mod 5$, the equation $x^5 + y^5 = 2\beta z^p$ has no non-trivial primitive solutions.

5.2. The case $3 \mid d$. In this case $a + b$ may be odd. Hence we also need to consider level 800, but in our favor we have $3 \mid a + b$. We compute the spaces $S_2(M, \epsilon)$ with $M = 1600, 800, 400$ or 100 and again divide them into the sets $S_1, S_2$ and $S_3$. This time we will also need to make some further subdivisions according to the parity of $a + b$ and the level that will become clear below. Let $\mathfrak{p}_3$ be the prime of $K$ above 3 and note that for $a + b$ odd the possible levels are only 800 or 1600.

**Newforms in S2:** We use the same type of argument as for $2 \mid d$. Indeed, we already know that $a_3(S_1) = t - it$, with $t \in \mathbb{Z}$ such that $|t| \leq 2$. Again, if $f = q + \sum_{n \geq 2} c_n q^n$ is a newform in $S_2$ such that $\bar{\rho} \sim \bar{\rho}_f, \mathfrak{p}_3$, then the congruence

$$a_3(S_1) \equiv a_3(f) \pmod{\mathfrak{p}_3}$$

must hold. In particular, there is a newform in $S_2$ having $a_3(f)$ with minimal polynomial $x^2 \pm (2 - 2i)x + i$. We now apply the minimal polynomial of $a_3(f)$ to both sides of the congruence above and then replace $t$ by all its possible values to find a contradiction with $p > 73$. By repeating this process for all forms in $S_2$ we find that $3$ works as a bound for all cases.

**Newforms in S3:** Recall that $\rho|_{G_K} = \rho_{E_{\gamma}, p}$. Suppose now that $\bar{\rho} \sim \bar{\rho}_f, \mathfrak{p}$ for some newform $f$ in $S_3$; in particular, $\bar{\rho}|_{G_K} \sim \bar{\rho}_f, \mathfrak{p} \mid_{G_K}$. Observe that by Proposition 5.8 the number $a_{\mathfrak{p}_3}(f) = \text{tr}(\rho|_{Frob_{\mathfrak{p}_3}}(\rho|_{G_K}))$ is a rational integer. By evaluating both sides in the previous isomorphism at $\text{Frob}_{\mathfrak{p}_3}$ and taking traces we see that

$$a_{\mathfrak{p}_3}(E) \equiv a_{\mathfrak{p}_3}(f) \pmod{p}.$$
On one hand, for a prime $\mathfrak{p}$ of good reduction for $E_\gamma$, the quantity $a_{\mathfrak{p}}(E_\gamma)$ is equal to $l^s + 1 - \# E_\gamma(\mathbb{F}_l)$, where $l^s$ is the number of elements of the residue field at $\mathfrak{p}$ and $E_\gamma$ is the elliptic curve obtained by reducing $E_\gamma$ modulo $\mathfrak{p}$. Using SAGE it is easy to check by direct computation that the hypothesis $3 \mid a + b$ implies that $E_\gamma \mod \mathfrak{P}_3$ is the same for any pair $(a,b)$ and that $E_\gamma$ has $a_{\mathfrak{P}_3}(E_\gamma) = -18$ for all $a, b$. On the other hand, looking for the $a_3(f)$ coefficients of the newforms of type S3 we find four possibilities $\pm(2i-2)$ and $\pm(i-1)$. It is known that if $\alpha, \beta$ are the roots of the polynomial $x^2 - a_3(f)x + \epsilon(3)3$ (the characteristic polynomial of $\rho_{f,3}(\text{Frob}_3)$), then $a_{\mathfrak{P}_3}(f) = \alpha^3 + \beta^3$. Since $\epsilon(3) = -i$, by substituting for each of the four values of $a_3(f)$ we find that $a_{\mathfrak{P}_3}(f) = 14$ or 2. Hence $\hat{\rho} \sim \tilde{\rho}_{f,3}$ is not possible if $p > 3$.

**Newforms in S1:** The newforms with complex multiplication by $\mathbb{Q}(\sqrt{-5})$ verify $a_3(f) = \pm(i - 1)$. Then we use the argument we have just described to get a contradiction with $3 \mid a + b$. Thus we have to eliminate only newforms with CM by $\mathbb{Q}(i)$, and for that we use the same argument as for $2 \mid d$. For $p > 13$, if we suppose that $p$ splits in $\mathbb{Q}(i)$, i.e. $p \equiv 1 \pmod{4}$, we have a contradiction with Proposition 3.4 in [7].

**Newforms in S2:** Since we have considered separately the newforms of level 800, the set $S2$ that we are considering now is a subset of the one considered in the case $2 \mid d$. Also, we are assuming $p > 73$. Then the exact same argument as for $2 \mid d$ holds, i.e. the argument in section 5.1 in the paragraph starting with “Newforms in S2:...”.

**Newforms in S3:** For $f$ in S3 we first twist them by the Dirichlet character of $\mathbb{Q}(\sqrt{2})$, and we already know that $f \otimes \chi$ is a newform of level 800. On the other hand we twist the Frey curve $E_\gamma(a,b)$ by the same character. If the conductor of $f$ is 2 of the twisted curve is not $2^5$, we have a contradiction via Carayol as in the case $2 \mid d$; if it is $2^5$, then since $E_\gamma \otimes \chi$ modulo $\mathfrak{P}_3$ is equal to $E_\gamma(a,b) \mod \mathfrak{P}_3$, we are in the same situation as above (with forms of level 800 and type S3), and the arguments used there with the values of $a_{\mathfrak{P}_3}(E_\gamma)$ and $a_{\mathfrak{P}_3}(f)$ gives us the desired contradiction.

**$a+b$ even and any level:** In this case $6 = 2 \times 3 \mid a + b$. Then all the arguments described for both $2 \mid d$ and $3 \mid d$ can be used. For newforms of types S2 and S3 we apply exactly the same arguments used in section 5.1 for $2 \mid d$ but with $p > 73$. For newforms of type S1 we only need to suppose that $p \equiv 1 \pmod{4}$ to get a contradiction. As we already observed, this is because the newforms with CM by $\mathbb{Q}(\sqrt{-5})$ satisfy $a_3 = \pm(i - 1)$, which contradicts $3 \mid a + b$. Up to now we have just proved

**Theorem 5.2.** For any $p > 73$ such that $p \equiv 1 \pmod{4}$, the equation $x^5 + y^5 = 3\beta z^p$ has no non-trivial primitive solutions.

5.3. The multi-Frey approach. In this section we end the proof of Theorem 1.3 and 1.2 via the Siksek multi-Frey technique. As its name suggests, the multi-Frey approach is a modular approach which makes use of more than one Frey-curve. This technique was introduced by Siksek in [14] and further generalized in [5]. The main observation is that if we have $n$ distinct modular Frey-curves $E_i$ for $2 \leq i \leq n$ attached to a putative solution $(a,b,c)$, then this will imply several simultaneous isomorphisms between the Galois representations $\rho_{E_i,p}$ and the
representations $\bar{\rho}_{f,\mathfrak{p}}$, attached to their corresponding modular forms. In general, this should allow us to give a better bound for the exponent $p$ in $\square$.

We start by giving a second Frey-curve. From the relation
\[
\left(-\frac{3}{10}\sqrt{5} + \frac{1}{2}\right)\phi_1 + \left(\frac{3}{10}\sqrt{5} + \frac{1}{2}\right)\phi_2 = (a - b)^2
\]
we can consider the curves $F_{(a,b)}$ also defined over $\mathbb{Q}(\sqrt{5})$ and given by
\[
F = F_{(a,b)} : y^2 = x^3 + 2(a - b)x^2 + \left(-\frac{3}{10}\sqrt{5} + \frac{1}{2}\right)\phi_1(a,b)x.
\]

We have checked that these are $\mathbb{Q}$-curves, and after applying Quer’s theory analogously to what we did for $E_{(a,b)}$, we find that the same splitting character/field and twist $\gamma$ computed previously also work for $F$. After computing the conductor of $F_{\gamma}/K$, applying Milne’s formula and Serre’s conjecture we find that we need to eliminate newforms with level 100, 400 or 1600 if $8 \parallel a + b$, 4 \parallel a + b or 2 \parallel a + b, respectively. Also, if $2 \nmid a + b$ we can suppose that $a$ is even and we are in level 800 or 1600 if $4 \mid a$ or $4 \nmid a$, respectively. Moreover, it also follows from the conductor of $F_{\gamma}$ that if $l \nmid 2, 5$ is a prime in $K$ of bad reduction for $F_{\gamma}$, then $l$ must divide $\phi(a,b)$.

We now recall that, in the previous sections, when working with $E_{\gamma}$ we needed to eliminate newforms with level 400, 100 or 1600 if $8 \mid a + b$, 4 \parallel a + b or 2 \parallel a + b, respectively. Also, when $2 \nmid a + b$ and $a$ is even, we were in level 800 or 1600 depending if $4 \mid a$ or $4 \nmid a$, respectively. Thus interchanging $E_{\gamma}$ by $F_{\gamma}$ only switches the levels 100 and 400. The reason for this observation will be clear below.

To apply the multi-Frey technique with the curves $E_{(a,b)}$ and $F_{(a,b)}$ we first need to give the definitions according to our case. For that we will need

**Proposition 5.3.** Let $f$ be one of the computed newforms with coefficient field $\mathbb{Q}_f = \mathbb{Q}(i)$. Let $\mathfrak{p}$ be a prime in $K = \mathbb{Q}(\theta)$. Then $a_{\mathfrak{p}}(f) = \text{tr}(\rho_{f,\lambda}|_{G_K}(\text{Frob}_{\mathfrak{p}}))$ is an integer number.

**Proof.** Since the nebentypus $\bar{\epsilon}$ fixes $K$ and $f$ has an inner-twist by $\bar{\epsilon}$, it is known that the traces of Frobenius of $\rho_{f,\lambda}|_{G_K}$ are algebraic integers in a totally real subfield of $\mathbb{Q}_f$. From $\mathbb{Q}_f = \mathbb{Q}(i)$ it follows trivially that $a_{\mathfrak{p}}(f) \in \mathbb{Z}$.

Recall that $K = \mathbb{Q}(\theta)$ is of degree 4, and for an inert prime $q$ denote by $\mathfrak{q}_q$ the only prime of $K$ above $q$. Let $q \in \mathbb{Z}$ be a prime inert in $K$ of good reduction to both families $E_{(a,b)}$, $F_{(a,b)}$. Given a newform $f$, if $\alpha, \beta$ are the roots of the characteristic polynomial of $\rho_{f,\mathfrak{q}}(\text{Frob}_q)$, i.e. $x^2 - a_q(f)x + \bar{\epsilon}(q)q$, then $a_{\mathfrak{q}_q}(f) = \alpha^4 + \beta^4$ (in the previous section, in the sub-case corresponding to $a + b$ odd and level 800, we used this for $q = 3$). From Proposition 5.3 we know that $a_{\mathfrak{q}_q}(f)$ is an integer. Now, given a newform $f$ satisfying the hypothesis of Proposition 5.3 and a non-zero pair $(x, y) \in {\mathbb{F}_q}^4 \times {\mathbb{F}_q}^4$, we define the following quantities:

\[
E_{(x,y)}(q,f) := a_{\mathfrak{q}_q}(E_{(x,y)}) - a_{\mathfrak{q}_q}(f),
\]
\[
F_{(x,y)}(q,f) := a_{\mathfrak{q}_q}(F_{(x,y)}) - a_{\mathfrak{q}_q}(f).
\]

Moreover, given a pair of such newforms $(f, g)$ we put
\[
A_q(f,g) := \prod_{(x,y) \in \mathbb{F}_q^4 \setminus \{(0,0)\}} \gcd(E_{(x,y)}(q,f), F_{(x,y)}(q,g)).
\]
Now, if \((a, b, c)\) is a primitive solution to (4) or (5) there is a pair of newforms \((f, g)\) and primes \(\mathfrak{p}\) and \(\mathfrak{p}'\) above \(p\) such that

\[
\begin{align*}
\bar{\rho}_{E,p} &\sim \bar{\rho}_{f,\mathfrak{p}}|G_K, \\
\bar{\rho}_{F,p} &\sim \bar{\rho}_{g,\mathfrak{p}'}|G_K.
\end{align*}
\]

Instead of eliminating newforms as in the previous section, we are now interested in eliminating pairs, and for that we will use information from both \(E\) and \(F\). For example, if both \(f, g\) have a coefficient field \(\mathbb{Q}(i)\) and \(q\) is a prime as above then, by evaluating the two isomorphisms above at \(\text{Frob}_{\mathfrak{p},q}\) and taking traces, we see that \(p \mid A_q(f, g)\). Thus we can eliminate a pair \((f, g)\) if \(A_q(f, g) \neq 0\) by imposing (for example) \(p > A_q(f, g)\). Note also that there is only a finite number of pairs to eliminate.

We will now finish the proofs of Theorems 1.1 and 1.2. Note that the differences between what we have already proved in the previous two sections and the statement of Theorems 1.1 and 1.2 are the congruence conditions on the exponent \(p\). Those conditions arise from Ellenberg’s theorem when eliminating the newforms with CM. We observe that in level 800 there are no newforms with CM and in level 1600 there are four corresponding to the elliptic curves \(E_{(1,1)}, F_{(1,1)}, E_{(1,-1)}\) and \(F_{(1,-1)}\). Let \(f_1, f_2\) denote the two forms with CM by \(\mathbb{Q}(i)\), and by \(g_1, g_2\) those with CM by \(\mathbb{Q}(\sqrt{-5})\). Let \(\chi\) be the character of \(\mathbb{Q}(\sqrt{2})\). On level 100 there are three newforms with CM, \(g_1 \otimes \chi, g_2 \otimes \chi, f_1 \otimes \chi\), and on level 400 there is \(f_2 \otimes \chi\). Since there are no newforms with CM in level 800, the argument that follows can be applied to both cases \(2 \mid d\) and \(3 \mid d\).

Given a primitive solution \((a, b, c)\) to (4) or (5) we have a double isomorphism as explained above:

\[
\begin{align*}
\bar{\rho}_{E,p} &\sim \bar{\rho}_{f,\mathfrak{p}}|G_K, \\
\bar{\rho}_{F,p} &\sim \bar{\rho}_{g,\mathfrak{p}'}|G_K,
\end{align*}
\]

where \(f \in S_2(M_f, \varepsilon)\) and \(g \in S_2(M_g, \varepsilon)\), where the pair of levels \((M_f, M_g)\) may be \((400, 100), (100, 400), (1600, 1600)\) or \((800, 800)\). We consider all the pairs \((f, g)\) of newforms respecting the previous pairs of levels, and we divide them in two sets: let \(SS_1\) be the set of pairs \((f, g)\) where \(f\) has no CM and \(SS_2\) be the set of those where \(f\) has CM. We eliminate a pair \((f, g)\) in \(SS_1\) by applying the arguments on \(f\) explained in the previous two sections. For pairs \((f, g)\) in \(SS_2\) such that \(g\) has a coefficient field strictly containing \(\mathbb{Q}(i)\), we eliminate them by applying to \(g\) the exact same argument as in the previous two sections in the subcase Newforms in \(S_2\). We are left with pairs in \(SS_2\) such that both forms have a coefficient field \(\mathbb{Q}(i)\). Note that \(q = 3, 7, 13, 17\) satisfy \(q \neq 1 \pmod{5}\) and hence by Corollary 2.5 \(q \mid \phi(a, b)\); thus it is of good reduction to both families \(E_{(a,b)}\) and \(F_{(a,b)}\). Given \((f, g)\) in \(SS_2\) such that both \(f, g\) have coefficient field \(\mathbb{Q}(i)\), we compute \(A_q(f, g)\) using the auxiliary primes \(q = 3, 7, 13, 17\) to find that \(A_q(f, g) = 0\) for all the auxiliary primes only if \(f, g\) have CM by distinct fields. Moreover, when \(A_q(f, g) \neq 0\) we check that all prime factors of \(A_q(f, g)\) are \(\leq 13\). Hence there are eight surviving pairs: \((f_1, g_1), (f_1, g_2), (g_1, f_1), (g_2, f_2), (g_1 \otimes \chi, f_2 \otimes \chi), (g_2 \otimes \chi, f_2 \otimes \chi), (f_2 \otimes \chi, g_1 \otimes \chi)\) and \((f_2 \otimes \chi, g_2 \otimes \chi)\). For a prime \(p \equiv 1 \pmod{4}\) or \(p \equiv \pm 1 \pmod{5}\) we can eliminate these pairs by conveniently applying Proposition 3.4 in [7] to \(E\) or \(F\). Thus Theorem 1.1 and Theorem 1.2 follow.
6. Finding $E_\gamma$

In this section we prove Theorem 3.2 by extensively using the work of Quer (see [11] and [12] for the notation and details). Theorem 3.2 will follow by a direct application of Theorem 5.4 in [11] to $E_\gamma$. We recall here the particular case of Quer’s theorem that we need.

**Theorem 6.1** (Quer). Let $C$ be a $\mathbb{Q}$-curve without complex multiplication completely defined over a minimal splitting field $K$ and such that $\xi_K(C)$ has trivial Schur class. Let $\epsilon$ be a splitting character for $\xi_K(C)$. Let $\{a_i\}$ and $\{d_i\}$ be dual bases with respect to the degree map corresponding to $C$, which we assume to be chosen as usual if $K_{\epsilon} \cap K_d$ is a quadratic field.

Then, if $\epsilon$ has order 4, $K_{\epsilon} \cap K_d = \mathbb{Q}(\sqrt{a_1})$ and $d_1 = 2$, then the abelian variety $B$ decomposes over $\mathbb{Q}$ as a product of two non-$\mathbb{Q}$-isogenous abelian varieties of $GL_2$-type, both of them with a $\mathbb{Q}$-endomorphism algebra isomorphic to $\mathbb{Q}(\zeta_8, \sqrt{2}, \sqrt{d_2}, ...)$.

We now proceed to show that $E_\gamma$ is in the conditions of this theorem. First note that the theory of Quer always requires curves without complex multiplication. Hence we need

**Theorem 6.2.** Let $(a, b, c)$ be a primitive non-trivial solution of equation (4) or (5). Then the curve $E = E_{(a, b)}$ has no complex multiplication.

**Proof.** This theorem follows immediately from the fact that the primes dividing $c$ are of semistable reduction of $E$. □

The minimal field of definition of $E$ is $K_d = \mathbb{Q}(\sqrt{5})$, and $\{a_1\} = \{5\}$, $\{d_1\} = \{2\}$ is a dual base respect to the corresponding degree map. Since the quaternion algebra $(5, \pm 1) \neq 1$ from Proposition 4.3b of [11], we know that $K_d$ is not a splitting field. Let $L = \mathbb{Q}(\sqrt{5}, \sqrt{-2})$ be a biquadratic field of complete definition of $E$ (i.e. a field where all the conjugates of $E$ and isogenies between them are defined) and let $\sigma, \tau \in Gal(L/\mathbb{Q})$ be such that

\[
\begin{cases}
\sigma(\sqrt{5}) = \sqrt{5} & \text{and} & \sigma(\sqrt{-2}) = -\sqrt{-2}, \\
\tau(\sqrt{5}) = -\sqrt{5} & \text{and} & \tau(\sqrt{-2}) = \sqrt{-2}.
\end{cases}
\]

From the explicit expression for the isogeny in section 3 we compute the 2-cocycle

$\phi_L(g, h) = \phi_g \phi_h \phi_{gh}^{-1}$

obtaining

**Table 2. Values of $c_L$**

<table>
<thead>
<tr>
<th>$g$</th>
<th>$h$</th>
<th>$\sigma$</th>
<th>$\tau$</th>
<th>$\sigma \tau$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>\sigma</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>\tau</td>
<td>1</td>
<td>1</td>
<td>-2</td>
<td>-2</td>
</tr>
<tr>
<td>\sigma \tau</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
From Table 2 we see that $c_K(\sigma, \tau) \neq c_K(\tau, \sigma)$. Hence we cannot find a splitting map $\text{Gal}(L/\mathbb{Q}) \to \mathbb{Q}^*$ such that

$$c_K(g, h) = \frac{\beta(g)\beta(h)}{\beta(gh)},$$

and hence $L$ does not contain a splitting field for $\xi(C)$. We need to find an appropriate splitting character in order to have a splitting field and apply Proposition 5.2 in [11]. First by Theorem 3.1 in [11] one sees that $\xi(C)_\pm = (5, 2)$. Using Theorem 4.2 in [11] and local information it can be checked that the character $\epsilon : (\mathbb{Z}/20\mathbb{Z})^* \to \mathbb{Q}(\zeta_4)$ of order 4 and conductor 20 given by

$$(9) \quad \epsilon = \epsilon_2 \epsilon_5,$$

where $\epsilon_2$ is the quadratic character of conductor 4 and $\epsilon_5$ is the character of order 4 and conductor 5 given by $\epsilon_5(2) = \zeta_4 = i$, is an appropriate splitting character. Its fixed field is $K_\epsilon = \mathbb{Q}(\theta)$, where $\theta = \sqrt{\frac{1}{2}(5 + \sqrt{5})}$. Then it follows from Proposition 5.2 in [11] that there is a representative in the isogeny class of $E$ which is completely defined over $K_\beta = K_\epsilon K_d = \mathbb{Q}(\theta)\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\theta)$ and has trivial Schur class. We denote it by $E_\gamma$.

Now we will explicitly solve an embedding problem to find $\gamma$. As explained in section 3 of [12], let

$$(10) \quad \xi_{K_\beta L} = (\text{Inf}^\text{Gal}(K_\beta L/\mathbb{Q}) c_{K_\beta}(E_\gamma))\pm (\text{Inf}^\text{Gal}(K_\beta L/\mathbb{Q}) c_{L}(E))\pm$$

after the identification with an element of $H^2(K_\beta L/\mathbb{Q}, \{\pm 1\})$. The embedding problem associated with $\xi_{K_\beta L}$ is unobstructed and admits solutions $\gamma \in K_\beta$. Applying Theorem 3.1 in [12] will hold one of these solutions, but first we need to restate our embedding problem in a way compatible with the notation of the theorem. Note that $c_{L}(E)_\pm = c_{A,B}$ with $A = \{-10\}$ and $B = \{5\}$, where $c_{L}(E)_\pm$ is given by the signs in Table 2.

Let $\xi_{A,B}$ and $\theta_\epsilon$ be as in [12], where the character $\epsilon$ is the one above. Now using to the notation of Theorem 3.1 in [12] we consider the decomposition

$$K = \mathbb{Q}(\theta, \sqrt{-2}) = LMN = \mathbb{Q}(\theta)\mathbb{Q}(\sqrt{-10})\mathbb{Q},$$

which gives $e = 1$ ($L \cap M = \mathbb{Q}$), $m = 1$ and $s = 0$, and let $\sigma_0, \sigma_1 \in \text{Gal}(K/\mathbb{Q})$ reflect this decomposition. That is,

$$\left\{ \begin{array}{ll}
\sigma_0(\sqrt{5}) = -\sqrt{5} \quad & \text{and} \quad \sigma_0(\sqrt{-2}) = -\sqrt{-2}, \\
\sigma_1(\sqrt{5}) = \sqrt{5} \quad & \text{and} \quad \sigma_1(\sqrt{-2}) = -\sqrt{-2}.
\end{array} \right.$$  

We put $c = \xi_{A,B}\theta_\epsilon$ and compute $\zeta = c(1, \sigma_0)c(\sigma_0, \sigma_0)c(\sigma_0^2, \sigma_0)c(\sigma_0^3, \sigma_0) = -1$. Theorem 3.1 in [12] says that the embedding problem $(K/\mathbb{Q}, \{\pm 1\}, [c])$ is solvable if and only if we can find elements $\alpha_0, \alpha_1$ such that

$$N_{\sigma_0}(\alpha_0) = -1,$$

$$N_{\sigma_1}(\alpha_1) = 5,$$

$$\frac{\sigma_1\alpha_0}{\alpha_0} = \frac{\sigma_0\alpha_1}{\alpha_1}.$$
Since \( c = \xi_K L \) (here we are using notation of equation (10)) we already know that this problem is unobstructed, and a small search leads us to
\[
\alpha_0 = \frac{1}{2}(-1 + \theta + \theta^2)\sqrt{-2}, \\
\alpha_1 = -5 + 2\theta^2.
\]
Moreover, the same theorem gives us a splitting map for the cocycle \( c \) given by
\[
\beta_{\text{id}} = \beta_{\sigma_1} = 1, \\
\beta_{\sigma_0} = \beta_{\sigma_1 \sigma_0} = \alpha_0, \\
\beta_{\sigma_2}^0 = \beta_{\sigma_1 \sigma_2} = 2 - \theta - \theta^2, \\
\beta_{\sigma_3} = \beta_{\sigma_1 \sigma_3} = \frac{\sqrt{-2}}{2}(-\theta^2 - \theta + 3).
\]
Finally, taking \( x = 1/4 \) in formula (1) in [12] we conclude that \( \gamma = 2\theta^2 - \theta - 5 \in K \) is a solution. Now a direct application of Theorem 5.4 in [11] to \( E_\gamma \) yields Theorem 3.2.

\[\square\]

ACKNOWLEDGMENTS

The authors want to thank Nicolas Billerey for the discussions regarding the construction of the \( \mathbb{Q} \)-curves in section 3. We also thank the anonymous referee for pointing out the existence and relevance of an extra Frey-curve (\( F_{(a,b)} \)) in section 5.3 attached to solutions of (1).

REFERENCES

FERMAT-TYPE EQUATIONS SOLVED THROUGH Q-CURVES

DEPARTMENT OF ALGEBRA AND GEOMETRY, UNIVERSITY OF BARCELONA, GRAN VIA DE LES CORTS CATALANES, 585, 08007 BARCELONA, SPAIN

DEPARTMENT OF ALGEBRA AND GEOMETRY, UNIVERSITY OF BARCELONA, GRAN VIA DE LES CORTS CATALANES, 585, 08007 BARCELONA, SPAIN