THE DIOPHANTINE EQUATION $A^4 + 2^\delta B^2 = C^n$

MICHAEL A. BENNETT, JORDAN S. ELLENBERG AND NATHAN C. NG

1. Introduction

In [10], the second author proved that the equation

$$A^4 + B^2 = C^p \tag{1}$$

had no integral solutions for prime $p > 211$ and $AB \neq 0$. In the present paper, we explain how to extend this result to smaller exponents, and to the related equation

$$A^4 + 2B^2 = C^p. \tag{2}$$

In addition to the intrinsic interest of generalized Fermat problems, the analysis of these equations provides a good test of contemporary Diophantine techniques; in the present paper we use a combination of modularity of Galois representations, averaging arguments from analytic number theory, and Chabauty methods in order to control integral solutions to (1) and (2). These two equations also arise rather curiously in recent work of the first author and Mignotte [1], related to a classification of prime q such that congruent number curves of the shape

$$Y^2 = X^3 - N^2 X, \quad N = 2^\alpha q^\beta$$

possess nontrivial integral points.

In [10], one already has that (1) has no nontrivial solutions whenever there exists a modular form f in a certain Atkin-Lehner eigenspace of $S_2(\Gamma_0(2p^2))$ or $S_2(\Gamma_0(p^2))$ satisfying $L(f \otimes \chi_{-4}, 1) \neq 0$, where χ_{-4} is the Dirichlet character of conductor 4; furthermore, the results of [10] show that such a form exists for p (effectively) large enough. To check the remaining values of p is in principle a finite computation, but computing in the space of newforms of level $2p^2$ is still difficult when p is on the order of 211. In the present paper, we prove the following theorem :

Theorem 1. *There are no solutions to the equation $A^4 + B^2 = C^n$ with $AB \neq 0$ and $n \geq 4$. The only solution to the equation $A^4 + B^2 = C^n$ and $A^4 + 2B^2 = C^n$ with $AB \neq 0$ and $n \geq 4$ is $(A, B, C, n) = (1, 11, 3, 5)$.*

The first part of the paper is a sharpening of the analytic bounds used in [10] in order to prove Theorem 1 whenever n is a prime at least 61 (for the first equation) and at least 97 (for the second.) In the second part, we deal with the remaining n on a case by case basis. We hope that the paper will provide an instructive example of the interplay between analytic, geometric, and computational techniques in Diophantine equations.

2. Preliminaries

We first recall the main ideas of [10] (see also [7]). If $A^4 + B^2 = C^p$, the curve

$$E_{A,B} : y^2 = x^3 + 2(1+i)Ax^2 + (B + iA^2)x \tag{3}$$

is a $\mathbb{Q}$-curve, which is to say its Galois conjugates are isogenous to one another. It follows that there is a mod p Galois representation $\bar{\rho}_{E,p} : G_{\mathbf{Q}} \to GL_2(\bar{\mathbf{F}}_p)$ attached to $E := E_{A,B}$. By Lemma 4.3 of [10], one knows that E has potentially multiplicative reduction at some prime greater than 3 (under the assumption that $AB \neq 0$.) Lemma 4.4 and Proposition 4.5 of [10] then show that $\bar{\rho}_{E,p}$ is either reducible or is equal to the mod p representation attached to a newform of weight 2 and level 32 or 256.

Similarly, recent work of Dieulefait and Jiménez [7] shows that if (A, B, C) is a solution to $A^4 + 2B^2 = C^p$, the $\mathbb{Q}$-curve

$$E_{A,B} : y^2 = x^3 + 4Ax^2 + 2(A^2 + \sqrt{-2}B)x \tag{4}$$

again yields a representation $\bar{\rho}_{E,p} : G_{\mathbf{Q}} \to \mathrm{PGL}(\bar{\mathbf{F}}_p)$. Again, $E_{A,B}$ is modular (see the discussion after Theorem 2 in [7].) So $\bar{\rho}_{E,p}$ is either reducible or is a modular representation attached to a newform of weight 2 and level 256 or 512. (For a discussion of the applicability of this method to equations of the form $A^4 + dB^2 = C^p$, see [11].)

The newforms of levels 32 and 256 are all CM. In level 512, there are non-CM forms. As Dieulefait and Jiménez point out, however, these non-CM forms do not have the same inner twist as does $\bar{\rho}_{E,p}$; if $\bar{\rho}_{E,p}$ is the mod-p representation attached to some such f, this is a strong constraint on p. More precisely: one checks that the non-CM forms of level 512 have $a_3(f) = \sqrt{2}$ or $a_3(f) = \sqrt{6}$. However, $a_3(E_{A,B})$ must be an integer, since 3 splits in $\mathbb{Q}(\sqrt{-2})$. Thus p divides the norm of either $n - \sqrt{2}$ or $n - \sqrt{6}$ for some integer n with $|n| \leq 2\sqrt{3}$, and this implies that p is at most 7. In essence, this argument dates back to work of Serre [17].

We conclude that if $p > 7$ (or even if $p = 7$ in case E is as given in (3)), then $\bar{\rho}_{E,p}$ is either reducible or is congruent to a CM representation, which in particular implies that its image lies in the normalizer of a Cartan subgroup. In most of these cases, the theorems of [10] will show that $E_{A,B}$ has potentially good reduction at all primes not dividing 6, contradicting the following lemma.

Lemma 2. *$E_{A,B}$ has potentially multiplicative reduction at some prime greater than 3.*

Proof. This is proved in [10, Lemma 4.3] in the case of (1), and in [7] in the case of (2); we include a separate argument here only to handle the case where C is a power of 3 and p is small. For such a situation, this amounts to finding all S-integral points on curves of the shape

$$y^2 + 2x^4 = 3^\delta,$$

for $S = \{3, \infty\}$ and $\delta \in \{0, 1, 2, 3\}$. This is nowadays relatively routine; using the Magma command $SIntegralLjunggrenPoints([1, -2, 0, 3^\delta], [3])$ leads to the conclusion that

$$A^4 + 2B^2 = 3^n$$

with A, B positive integers implies

$$(A, B, n) = (1, 1, 1), (5, 1, 3), (1, 11, 5).$$

□

If $p > 13$, it now follows from [10] and [7] that $\bar{\rho}_{E,p}$ is in fact irreducible.

Lemma 3. *If $p = 7, 11, 13$ then $\bar{\rho}_{E,p}$ is irreducible.*

Proof. If $p = 11$ this follows from Proposition 3.2 of [10]. If $p = 7$, then E yields a K-point on the genus 1 modular curve $X_0(14)$ (where $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$ with the property that $P^\sigma = w_2 P$; in particular, it yields a point on $X_0(14)$ which projects to a rational point of $X_0(14)/w_2$. This quotient is an elliptic curve whose Mordell-Weil group is finite of order 6; the preimages of these points are all defined over $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{-7})$ (see [12]). So P must be a w_2-fixed point of $X_0(14)(\mathbb{Q})$; but w_2 acts without fixed points, so we are done. It is perhaps amusing to note that the non-CM points of $X_0(14)/w_2$ whose preimages in $X_0(14)$ lie in $\mathbb{Q}(\sqrt{-7})$ do, as expected, yield an interesting ternary identity; namely

$$7 + 181^2 = 2^{15}.$$

When $p = 13$, the curve E yields a rational point on $X_0(26)/w_2$, which is an elliptic curve of rank 0 with exactly three rational points; two of these lie under the cusps of $X_0(26)$, and the other under a pair of points over $\mathbb{Q}(\sqrt{13})$ parametrizing curves with CM by $\sqrt{-13}$. Since none of these points of $X_0(26)$ are noncuspidal points defined over K, we are done. □

We conclude that if $p > 7$ (or $p \geq 7$ for E as in (3)), then $\bar{\rho}_{E,p}$ has image contained in the normalizer of a Cartan subgroup.

In order to save ourselves some casework later on, we note that the case where $p \equiv 1 \pmod 8$ is easy to rule out.

Proposition 4. *Suppose $p \equiv 1 \pmod 8$. Then $\bar{\rho}_{E,p}$ does not have image contained in the normalizer of a Cartan subgroup.*

Proof. We have already observed that when $p > 7$, the representation $\bar{\rho}_{E,p}$ is the mod p reduction of a CM representation of conductor dividing 512. What's more, the CM field attached to this representation is either $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$. Since $p \equiv 1 \pmod 8$, both of these fields are split over p, and the CM representations have their images in the normalizer of a split Cartan subgroup. But this is impossible by Proposition 3.4 of [10]. □

As shown in [10], we can show that $\bar{\rho}_{E,p}$ is surjective as long as there exists a modular form in level p^2 or $2p^2$ with certain properties, which we record below. We write

$$\chi_d = \chi_d(n) = \left(\frac{d}{n}\right)$$

for the Kronecker symbol (we will be interested only in $d = -4$ or -8).

Proposition 5. *Let $p > 5$ be prime, and suppose there exists either*

- *a p-new form in $S_2(\Gamma_0(2p^2))$ with $w_p f = f$ and $w_2 f = -f$; or*

- *a p-new form in $S_2(\Gamma_0(p^2))$ with $w_p f = f$,*

such that $L(f \otimes \chi_{-4}, 1) \neq 0$. Then the mod p representation attached to a nontrivial solution of $A^4 + B^2 = C^p$ does not have image contained in the normalizer of a Cartan subgroup. Similarly, if there exists a newform f in one of the above two spaces satisfying $L(f \otimes \chi_{-8}, 1) \neq 0$, then the mod p representation attached to a nontrivial solution of $A^4 + 2B^2 = C^p$ does not have image contained in the normalizer of a Cartan subgroup.

Proof. This is essentially the discussion following Proposition 3.9 of [10]. We observe that the argument there, though given only for nonsplit Cartan subgroups, applies equally well to the split and nonsplit case. The split case can be handled by Proposition 3.4 of [10] when $p > 13$, so the point of this observation is merely to avoid having to treat $p = 13$ separately. □

This allows us immediately to handle (1) and (2) for many n merely by exhibiting weight 2 cuspforms with suitable properties. In fact, the great majority of Theorem 1 is a consequence of the following :

Proposition 6. *For each character χ_{-4} and χ_{-8}, and each prime $p > 7$ with $p \not\equiv 1 \pmod 8$, there exists a weight 2 cuspform f of level p^2 or $2p^2$ satisfying the criteria of Proposition 5. There exists a modular form f of level 98 satisfying the criteria of Proposition 5 for the character χ_{-4} of conductor 4.*

With this Proposition in hand, it remains to treat the equations

$$A^4 + B^2 = C^n, \quad n \in \{4, 5, 6, 9\} \tag{5}$$

and

$$A^4 + 2B^2 = C^n, \quad n \in \{4, 5, 6, 7, 9\}. \tag{6}$$

By a result of Darmon and Granville (Theorem 2 of [6]), each of these has at most finitely many solutions in coprime positive integers (A, B, C). We will in fact deduce the following :

Proposition 7. *Equation (5) has no solutions in positive coprime integers, while the only such solution to equation (6) is $(A, B, C, n) = (1, 11, 3, 5)$.*

The layout of this paper is as follows. In the next few sections, we will prove Proposition 6 for suitably large p. Our arguments are essentially refinements of those given in [9] and [10], based upon estimation of exponential sums. In Section 7, we will complete the proof of Proposition 6 by tabulating modular forms with the desired properties for $7 \leq p \leq 59$ and character χ_{-4}, and for $11 \leq p \leq 89$ and character χ_{-8}. Finally, in Sections 8 and 9, we will prove Proposition 7, by explicitly determining the rational points on a number of related hyperelliptic curves.

3. Converting the problem to analytic number theory

In the next four sections, we will concentrate on proving Proposition 6 for $p \geq 61$ (in the case of character χ_{-4}) and for $p \geq 97$ (in the case of χ_{-8}). To carry this out, we will translate the problem to one of estimating exponential sums. We begin by

introducing some notation. If f is a modular form, we denote by $a_m(f)$ the m-th Fourier coefficient of the q-expansion of f, viz

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

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

$$(a_m, L_\chi)_N := \sum_{f \in \mathcal{F}} a_m(f) L(f \otimes \chi, 1) \tag{7}$$

Here we are thinking of both a_m and L_χ as linear functions on the space $S_2(\Gamma_0(N))$.

Moreover, for $M \mid N$, we let $(a_m, L_\chi)_N^M$ denote the contribution to $(a_m, L_\chi)_N$ of forms which are new at level M. We define $(a_1, L_\chi)_{p^2}^{p-new}$ to be $(a_1, L_\chi)_{p^2} - (a_1, L_\chi)_{p^2}^p$.

As explained in [10], the conditions of Proposition 5 hold for an odd prime p as long as

$$\left| (a_1, L_\chi)_{p^2}^{p-new} \right| > 0$$

We now outline our strategy for deducing the nonvanishing of $(a_1, L_\chi)_{p^2}^{p-new}$. In [9] and [10], it is proven that

$$(a_1, L_\chi)_{p^2} = 4\pi + O\left((\log p)^2 p^{-2}\right) \text{ and } (a_1, L_\chi)_{p^2}^p = O(p^{-1}), \tag{8}$$

where the implied constants are absolute and explicit. Consequently, we have

$$|(a_1, L_\chi)_{p^2}^{p-new}| \geq 4\pi - C_1 (\log p)^2 p^{-2} - C_2 p^{-1}$$

for explicit constants C_1 and C_2. For large p, it is clear that the dominant error term on the right hand side of this inequality is the expression $C_2 p^{-1}$. On the other hand, for small primes p (say $p < 500$), the larger error term turns out to be $C_1 (\log p)^2 p^{-2}$, due to the comparative size of C_1 relative to C_2. The most significant part of our argument will thus be the evaluation of $(a_1, L_\chi)_{p^2}$ and subsequent determination of a good constant for C_1. The approach used by the second author in [9] to evaluate (7) was a refinement of a lemma appearing in a paper of Duke [8]. This method employs the Petersson trace formula for coefficients of modular forms. In this section, we shall apply the same methods to evaluate (7), but we sharpen some of the estimates of [9] by specializing the argument to the characters of conductors 4 and 8.

We have recently learned that Michel and Ramakrishnan in forthcoming work have proven exact formulae for certain sums of type (7). It is likely that some of the estimates in this section may be improved through appeal to their work.

We now present our explicit results, beginning by outlining our lower bound for $(a_1, L_\chi)_{p^2}$. In [9], the second author derives the decomposition

$$(a_m, L_\chi)_N = 4\pi \chi(m) e^{-2\pi m/\sigma N \log N} - E^{(3)} + E_3 - E_2 - E_1 + (a_m, B(\sigma N \log N)) \tag{9}$$

where the summands are bounded by explicit functions of N, m, and the conductor of χ, which we denote by q. We will use the following bounds from [9] without change:

Proposition 8. *Suppose $N \geq 400$, and let σ be a real number with $\sigma \geq q^2/2\pi$. Then we have*

- $|(a_m, B(\sigma N \log N))| \leq 30(\frac{400}{399})^3 e^{2\pi} q^2 m^{3/2} d(N) N^{-(1/2+2\pi\sigma/q^2)}$;
- $|E_1| \leq \frac{16}{3}\pi^3 m^{3/2}\sigma(\log N) e^{-N/2\pi m\sigma \log N}$;
- $|E_3| \leq \frac{8}{3}\zeta^2(\frac{3}{2})\pi^3\sigma m^{3/2} d(N)(\log N) N^{-1/2} e^{-N/2\pi m\sigma \log N}$.

In the following sections we will present bounds for E_2 and $E^{(3)}$ that improve on those given in [9]. We recall from [9] that E_2 is defined by

$$E_2 = 8\pi^2\sqrt{m}\sum_{n=1}^{\infty}\frac{\chi(n)}{\sqrt{n}} e^{-2\pi n/x} \sum_{\substack{N|c \\ c>2\pi\sqrt{mn}}} c^{-1} S(m,n;c)\Big(J_1\left(\tfrac{4\pi\sqrt{mn}}{c}\right) - \tfrac{2\pi\sqrt{mn}}{c}\Big), \tag{10}$$

where J_1 is the Bessel function of order one, while

$$E^{(3)} = 16\pi^3 m \sum_{N|c} c^{-2}\mathcal{S}(c), \tag{11}$$

where

$$\mathcal{S}(c) = \sum_{n=1}^{\infty}\chi(n) e^{-2\pi n/\sigma N\log N} S(m,n;c). \tag{12}$$

See pages 541–544 of [9] where these formulae are derived. In each case

$$S(m,n;c) = \sum_{uv\equiv 1(c)} e\left(\frac{mu+nv}{c}\right)$$

denotes the Kloosterman sum.

We note that E_1 and E_3 are very small for $N \geq 400$. Moreover, for appropriately chosen σ, the quantity $(a_m, B(\sigma N \log N))$ is small in the ranges under consideration, for both conductors 4 and 8. It remains to control E_2 and $E^{(3)}$, for which the bounds given in [9] are insufficient for our purposes. We will instead derive refined bounds for E_2 and $E^{(3)}$. Here and henceforth, we employ the notation

$$\theta = e^{-2\pi/x} \text{ with } x = \sigma N \log N.$$

Proposition 9. *Suppose χ is a character of even conductor, $N \geq 400$, and $\sigma \geq \frac{q^2}{2\pi}$. Then*

$$\begin{aligned} |E_2| &\leq 64 q\phi(q)\pi^5 m^2\left(\tfrac{\zeta(2)}{6}N^{-2} + \tfrac{1}{\pi}(\zeta(3)\log(\tfrac{eN}{2}) - \zeta'(3))N^{-3}\right) \\ &+ 32\pi^5\zeta(\tfrac{7}{2})^2 m^{\frac{5}{2}} d(N) N^{-7/2}\left((\tfrac{N^2}{4\pi^2 m}+1)(1-\theta)^{-1} + (1-\theta)^{-2}\right) e^{-\frac{N}{2\pi\sigma m\log N}} \\ &+ \tfrac{512}{3}\zeta(\tfrac{11}{2})^2\pi^7 m^{7/2} d(N) N^{-\frac{11}{2}}(1-\theta^2)^{-3} . \end{aligned} \tag{13}$$

We will postpone the proof of this until the next section. The most significant error term in equation (9) is in fact $E^{(3)}$. We shall determine a bound for $E^{(3)}$ by proving several estimates for $\mathcal{S}(c)$. In [9], one finds upper bounds of the shape

$$|\mathcal{S}(c)| \leq \frac{2\phi(q) c\log(c)}{\pi} \quad \text{and} \quad |\mathcal{S}(c)| \leq d(c)(cm)^{\frac{1}{2}}(1-\theta)^{-1}.$$

In case $\chi = \chi_{-4}$ or χ_{-8}, we will sharpen the first of these by factors of 4 and $4\sqrt{2}$ respectively. In the case when $N = p^2$, we improve the second bound by exploiting the fact that $S(m, n; p^2)$ may be evaluated in an elementary fashion. These improvements are listed in the next proposition.

Proposition 10. *Let c be a natural number.*
(i) If $c \geq 400$ and $\chi = \chi_{-4}$, then

$$|\mathcal{S}(c)| \leq f_1(c) := \frac{c}{\pi}(\log c + K_1)$$

where $K_1 = 2.242$.
(ii) If $c \geq 400$ and $\chi = \chi_{-8}$, then

$$|\mathcal{S}(c)| \leq f_2(c) := \frac{c}{\pi}\left(\frac{\sqrt{2}\log c}{\theta} + K_2\right)$$

where $K_2 = 3.038$.
(iii) If $m = 1$, χ is a character of even conductor, and $p^2 \mid c$ for a prime p then

$$|\mathcal{S}(c)| \leq f_3(c) := \frac{1}{3}d(c)c^{1/2}g(\theta)$$

where

$$g(u) := \frac{u}{1-u^2} - \frac{u^p}{1-u^{2p}} + \frac{\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)u^j}{1-u^p} - \frac{\sum_{j=1}^{p-1}\left(\frac{2j}{p}\right)u^{2j}}{1-u^{2p}} \ . \tag{14}$$

(iv) If χ is a character of even conductor, we have

$$|\mathcal{S}(c)| \leq f_4(c) := d(c)(cm)^{1/2}(1-\theta^2)^{-1} \ .$$

We note that if $m = 1$ then the bound $f_3(c)$ is better than the bound $f_4(c)$ by approximately a factor of 3. We expect $g(\theta) \approx (1-\frac{1}{p})(1-\theta^2)^{-1}$ as the sums in (14) are small. This is since θ is close to 1 and thus the sums are approximately equal to a Dirichlet character summed over a full period. Numerically, this will prove significant when p is small.

We deduce from this

Corollary 11. *(i) For $m = 1$, $N = p^2$ and $\chi = \chi_{-4}$, we have*

$$|E^{(3)}| \leq 16\pi^3 \sum_{p^2 \mid c} \min\left\{f_1(c), f_3(c), f_4(c)\right\} c^{-2} \ .$$

(ii) For $m = 1$, $N = p^2$ and $\chi = \chi_{-8}$, we have

$$|E^{(3)}| \leq 16\pi^3 \sum_{p^2 \mid c} \min\left\{f_2(c), f_3(c), f_4(c)\right\} c^{-2} \ .$$

In bounding $E^{(3)}$, we shall apply our bounds for $f_1(c)$ and $f_2(c)$ for small c, and our bounds for $f_3(c)$ and $f_4(c)$ for large c. We will also have need of a (relatively standard) divisor sum bound; as with Proposition 9, we will delay proving this until a later section.

Lemma 12. *Let $u \geq 60000$; then*

$$h(u) := \sum_{n>u} \frac{d(n)}{n^{3/2}} \leq \frac{2\log u + 4\gamma + 4.4}{\sqrt{u}} \ .$$

Assuming for the time being that we are equipped with Propositions 9 and 10, and Lemma 12 (which will be proved in Sections 4, 5 and 6, respectively), we are now in position to provide an explicit bound for $E^{(3)}$. We will consider the cases $\chi = \chi_{-4}$ and $\chi = \chi_{-8}$ simultaneously by supposing we have a bound of the form $|\mathcal{S}(c)| \le \frac{c}{\pi}(A \log c + B)$ for positive constants A and B.

Proposition 13. *Suppose that $m = 1$, $N = p^2$, and we have a bound of the form*

$$|\mathcal{S}(c)| \le \frac{c}{\pi}(A \log c + B) \ . \tag{15}$$

Then

$$|E^{(3)}| \le \min\left\{\beta_{1a}(p^2), \beta_{1b}(p^2)\right\}$$

where, for $X \ge 2$

$$\beta_{1a}(p^2) = \frac{16\pi^2}{p^2}(A(\tfrac{1}{2}\log^2 X + \tfrac{1}{9}) + (A\log(p^2)+B)(\log X + \tfrac{8}{9})) + \frac{48\pi^3(1-\theta^2)^{-1}h(X)}{p^3} \ ,$$

$$\beta_{1b}(p^2) = \frac{16\pi^3}{p^3}\sum_{b \le X} \min\left\{\frac{bp}{\pi}(A\log(bp^2)+B), d(b)b^{1/2}g(\theta))\right\} b^{-2} + \frac{16\pi^3 g(\theta)h(X)}{p^3} \ .$$

Proof. We begin by showing that $\beta_{1b}(p^2)$ provides an upper bound for $|E^{(3)}|$. Let $X \ge 2$ be a parameter. We shall write each $c = p^2 b$ and split the sum into two parts, the first consisting of those $b \le X$, and the second sum consists of those $b > X$. For those $c = p^2 b$ with $b \le X$ we apply the minimum of the bound (15) and $f_3(c)$ and for those with $b > X$ we apply the bound $f_3(c)$. Thus we deduce that

$$\sum_{p^2|c} |\mathcal{S}(c)| c^{-2}$$
$$\le \frac{1}{p^4}\sum_{b \le X} \min\left\{\frac{bp^2}{\pi}(A\log(bp^2)+B), d(b)b^{1/2}pg(\theta))\right\} b^{-2} + \frac{g(\theta)}{p^3}\sum_{b>X}\frac{d(b)}{b^{\frac{3}{2}}} \ .$$

The bound for $\beta_{1b}(p^2)$ thus follows from this last bound and (11). The bound for $\beta_{1a}(p^2)$ is similar. Instead, we apply the bound (15) for small values of c and $f_4(c)$ for large values of c. As before, we have

$$\sum_{p^2|c} |\mathcal{S}(c)| c^{-2} \le \frac{1}{p^4}\sum_{b \le X}\frac{bp^2(A\log(bp^2)+B)}{\pi b^2} + \frac{3(1-\theta^2)^{-1}}{p^3}\sum_{b>X}\frac{d(b)}{b^{\frac{3}{2}}} \ .$$

Since we have the inequalities

$$\sum_{b \le X}\frac{\log b}{b} \le \frac{1}{2}\log^2(X) + \frac{1}{9} \ \text{ and } \ \sum_{b \le X}\frac{1}{b} \le \log(X) + \frac{8}{9}$$

for $X \ge 2$ we deduce the bound for $\beta_{1a}(p^2)$.

We are now prepared to prove our lower bounds for $(a_1, L_\chi)_{p^2}^{p-new}$. The calculations presented here were carried out in PARI/GP. Details are available from the authors on request.

Lemma 14. *Let p be prime. If either $\chi = \chi_{-4}$ and $p \ge 61$, or $\chi = \chi_{-8}$ and $p \ge 97$ then we may conclude that*

$$\left|(a_1, L_\chi)_{p^2}^{p-new}\right| > 0.5.$$

Proof. Note that, from equation (9), after invoking our bounds for $(a_m, B(\sigma p^2 \log(p^2)))$, E_1, E_2, and E_3, as given in Propositions 8 and 9, we have that

$$|(a_1, L_\chi)_{p^2} - 4\pi e^{-2\pi/\sigma p^2(\log(p^2))}| \leq \beta_0(p^2) + |E^{(3)}|$$

where

$$\begin{aligned}\beta_0(p^2) &= 90(\tfrac{400}{399})^3 e^{2\pi} q^2 p^{-(1+4\pi\sigma/q^2)} + \tfrac{32}{3}\pi^3\sigma(\log p)e^{-\frac{p^2}{4\pi\sigma\log p}} \\ &+ 64q\phi(q)\pi^5(\tfrac{\zeta(2)}{6}p^{-4} + \tfrac{1}{\pi}(\zeta(3)(\log\tfrac{ep^2}{2}) - \zeta'(3))p^{-6}) \\ &+ 96\pi^5\zeta(\tfrac{7}{2})^2 p^{-7}((\tfrac{p^4}{4\pi^2}+1)(1-\theta)^{-1} + (1-\theta)^{-2})e^{-\frac{p^2}{4\pi\sigma\log p}} \\ &+ 512\zeta(\tfrac{11}{2})^2\pi^7 p^{-11}(1-\theta^2)^{-3} \\ &+ 16\zeta^2(\tfrac{3}{2})\pi^3\sigma(\log p)p^{-1}e^{-\frac{p^2}{4\pi\sigma\log p}}.\end{aligned}$$

We may also write, from p. 779 of [10],

$$(a_1, L_\chi)^p_{p^2} = p(p^2-1)^{-1}((a_1, L_\chi)_p - \chi(p)p^{-1}(a_p, L_\chi)_p)\ .$$

By the argument leading to Lemma 3.13 of [10], as mentioned in the errata to [10], we have for $m = 1$ or p,

$$|(a_m, L_\chi)_p| \leq \left(8\pi + 32\zeta(3/2)^2\pi^2 p^{-3/2}\right)\sum_{n=1}^{\infty} d(n)n^{-1/2}e^{-2\pi n/q\sqrt{p}}\ . \tag{16}$$

Since $d(n) \leq \sqrt{3n}$ we have that the above sum is bounded by $\sqrt{3}(1-e^{-\frac{2\pi}{q\sqrt{p}}})^{-1}$ and thus $|(a_m, L_\chi)_p| \leq \beta_{2a}(p)$, where

$$\beta_{2a}(p) = \sqrt{3}(8\pi + 32\zeta(3/2)^2\pi^2 p^{-3/2})(1-e^{-\frac{2\pi}{q\sqrt{p}}})^{-1}\ .$$

We can give a slightly better bound by bounding just the terms in (16) with $n > 1000$. Applying $d(n) \leq \sqrt{3n}$ again and bounding the sum by an integral we conclude that $|(a_m, L_\chi)_p| \leq \beta_{2b}(p)$, where

$$\beta_{2b}(p) = (8\pi + 32\zeta(3/2)^2\pi^2 p^{-3/2})\left(\sum_{n=1}^{1000}\frac{d(n)}{\sqrt{n}}e^{-2\pi n/q\sqrt{p}} + \frac{q\sqrt{3p}}{2\pi}e^{-\frac{2\pi}{q\sqrt{p}}1000}\right)\ .$$

This second bound shall prove useful when we consider small primes p. Since we have $4\pi e^{-2\pi/\sigma p^2\log(p^2)} \geq 4\pi(1-\frac{\pi}{\sigma p^2(\log p)}) \geq 12.5653$, at least provided $p \geq 61$ and $\sigma \geq \frac{8}{\pi}$, it follows from (9) that

$$|(a_1, L_\chi)^{p-new}_{p^2}| \geq 12.5653 - \beta_0(p^2) - \min\{\beta_{1a}(p^2), \beta_{1b}(p^2)\} - \tfrac{1}{p-1}\min\{\beta_{2a}(p), \beta_{2b}(p)\}$$

where β_{1a} and β_{1b} are as given in Proposition 13, and β_0, β_{2a}, and β_{2b} are as stated above.

We begin with the case $\chi = \chi_{-4}$. We set $\sigma = \frac{10.4}{\pi}$ and we apply the inequality corresponding to β_{1a} in Proposition 13, with parameters $A = 1, B = K_1$ and $X = (\frac{\pi\sigma}{12\phi(4)})^2 p^2\log^2(p^2)$. We also invoke our bound for β_{2a} to obtain the inequalities

$$\begin{aligned}\beta_0(p^2) &\leq 0.0791\ldots\ , \\ \beta_{1a}(p^2) &\leq 7.6177\ldots\ , \\ \tfrac{1}{p-1}\beta_{2a}(p) &\leq 3.5545\ldots\ , \\ \left|(a_1, L_\chi)^{p-new}_{p^2}\right| &> 1.3138\ldots\ .\end{aligned}$$

for $p = 89$. These inequalities are obtained for all $p \geq 89$, since $\beta_0(p^2)$, $\beta_{1a}(p^2)$ and $\frac{1}{p-1}\beta_{2a}(p)$ are monotone, decreasing functions of p. For $p = 61, 67, 71, 73, 79$, and 83 we apply the inequalities corresponding to β_{1b} with parameter $X = 2000000$ and β_{2b} to conclude that

$$\begin{aligned} \beta_0(p^2) &\leq 0.3131\ldots\ , \\ \beta_{1b}(p^2) &\leq 9.0476\ \ldots\ , \\ \tfrac{1}{p-1}\beta_{2b}(p) &\leq 2.6024\ldots\ , \\ \left|(a_1, L_\chi)_{p^2}^{p-new}\right| &> 0.6019\ldots\ . \end{aligned}$$

In the conductor 8 case, we put $\sigma = \frac{41.6}{\pi}$ and appeal to the upper bound β_{1a} of Proposition 13 with parameters $A = \frac{\sqrt{2}}{\theta}$, $B = K_2$ and $X = (\frac{\pi\sigma}{12\phi(8)})^2 p^2 \log^2(p^2)$ and we apply the upper bound β_{2a} to find that

$$\begin{aligned} \beta_0(p^2) &\leq 0.1011\ldots\ , \\ \beta_{1a}(p^2) &\leq 6.7012\ldots\ , \\ \tfrac{1}{p-1}\beta_{2a}(p) &\leq 5.1957\ldots\ , \\ \left|(a_1, L_\chi)_{p^2}^{p-new}\right| &> 0.5671\ldots\ , \end{aligned}$$

for $p \geq 137$. For $p = 97, 101, 103, 107, 109, 113, 127$, and 131, we apply the upper bounds β_{1b} with $X = 2000000$ and β_{2b} to obtain

$$\begin{aligned} \beta_0(p^2) &\leq 0.4861\ldots\ , \\ \beta_{1b}(p^2) &\leq 7.4205\ldots\ , \\ \tfrac{1}{p-1}\beta_{2b}(p) &\leq 3.6872\ldots\ , \\ \left|(a_1, L_\chi)_{p^2}^{p-new}\right| &> 0.9713\ldots\ . \end{aligned}$$

Assuming the validity of Propositions 9 and 10, and Lemma 12, this completes the proof of Lemma 14.

4. Proof of Proposition 9

In the next three sections, we will give the proofs of the three technical results Propositions 9 and 10, and Lemma 12, used in the preceding section. We begin by proving Proposition 9. We start with the identity

$$\left|J_1(x) - \frac{x}{2} + \frac{x^3}{16}\right| \leq \frac{x^5}{384}$$

valid for $0 \leq x < 2\sqrt{2}$. This implies that

$$\left|E_2 + 8\pi^2\sqrt{m}\sum_{n=1}^{\infty}\frac{\chi(n)}{\sqrt{n}}e^{-2\pi n/x}\sum_{\substack{N|c \\ c>2\pi\sqrt{mn}}} c^{-1}S(m,n;c)\frac{(4\pi\frac{\sqrt{mn}}{c})^3}{16}\right| \leq E_2''' \qquad (17)$$

where

$$E_3''' = 8\pi^2\sqrt{m}\sum_{n=1}^{\infty}\frac{|\chi(n)|}{\sqrt{n}}e^{-2\pi n/x}\sum_{\substack{N|c \\ c>2\pi\sqrt{mn}}} c^{-1}|S(m,n;c)|\frac{(4\pi\frac{\sqrt{mn}}{c})^5}{384}\ . \qquad (18)$$

In the sum in (17), we swap order of summation to obtain

$$\Big|E_2 + 32\pi^5 m^2 \sum_{\substack{N|c \\ c>2\pi\sqrt{m}}} c^{-4} \sum_{n<\left(\frac{c}{2\pi}\right)^2 \frac{1}{m}} n\chi(n)\theta^n S(m,n;c)\Big| \le E_2''' \ .$$

By writing the inner sum as a sum over all n and subtracting $n > \left(\frac{c}{2\pi}\right)^2 \frac{1}{m}$ we obtain $|E_2 + E_2'| \le |E_2''| + E_2'''$ where

$$E_2' = 32\pi^5 m^2 \sum_{\substack{N|c \\ c>2\pi\sqrt{m}}} c^{-4} \sum_{n=1}^{\infty} n\chi(n)\theta^n S(m,n;c),$$

and

$$E_2'' = 32\pi^5 m^2 \sum_{\substack{N|c \\ c>2\pi\sqrt{m}}} c^{-4} \sum_{n>\left(\frac{c}{2\pi}\right)^2 \frac{1}{m}} n\chi(n)\theta^n S(m,n;c) \ .$$

We now proceed to bound E_2', E_2'', and E_2'''. We shall first bound E_2''. Note that the Weil bound for the Kloosterman sum is

$$|S(m,n;c)| \le d(c)(mc)^{1/2}, \tag{19}$$

whence, writing $J = [(N/2\pi)^2 m^{-1}] + 1$,

$$|E_2''| \le 32\pi^5 m^{\frac{5}{2}} \sum_{n=J}^{\infty} n\theta^n \sum_{N|c} d(c) c^{-7/2} \le 32\pi^5 m^{\frac{5}{2}} d(N) N^{-7/2} \zeta(7/2)^2 \sum_{n=J}^{\infty} n\theta^n \ .$$

Since

$$\sum_{n=J}^{\infty} n\theta^n = \theta^J \left(\frac{J}{1-\theta} + \frac{\theta}{(1-\theta)^2}\right) \le e^{-\frac{N}{2\pi\sigma m \log N}} \left(\frac{J}{1-\theta} + \frac{\theta}{(1-\theta)^2}\right),$$

we conclude that

$$|E_2''| \le 32\pi^5 \zeta(\tfrac{7}{2})^2 m^{\frac{5}{2}} d(N) N^{-7/2} \left(\left(\tfrac{N^2}{4\pi^2 m} + 1\right)(1-\theta)^{-1} + (1-\theta)^{-2}\right) e^{-\frac{N}{2\pi\sigma m \log N}}.$$

Next we bound E_2'''. By (18) and (19), we obtain

$$\begin{aligned} |E_3'''| &\le \tfrac{64}{3}\pi^7 m^{\frac{7}{2}} \sum_{n\ge 1} |\chi(n)| n^2 \theta^n \sum_{N|c, c>2\pi\sqrt{mn}} d(c) c^{-11/2} \\ &\le \tfrac{64}{3}\pi^7 m^{7/2} d(N) N^{-11/2} \zeta(\tfrac{11}{2})^2 \sum_{\substack{n=1 \\ n \text{ odd}}}^{\infty} n^2\theta^n \ . \end{aligned} \tag{20}$$

Since

$$\sum_{\substack{n=1 \\ n \text{ odd}}}^{\infty} n^2\theta^n = \frac{\theta(\theta^4 + 6\theta^2 + 1)}{(1-\theta^2)^3} \le \frac{8}{(1-\theta^2)^3},$$

for $0 \le \theta \le 1$, we deduce

$$|E_3'''| \le \tfrac{512}{3}\pi^7 \zeta(\tfrac{11}{2})^2 m^{\frac{7}{2}} d(N) N^{-11/2} (1-\theta^2)^{-3} \ .$$

Lastly we deal with E_2'. By opening the Kloosterman sum, we see that

$$E_2' = 32\pi^5 m^2 \sum_{N|c, c>2\pi\sqrt{m}} c^{-4} \mathcal{U}(c)$$

where

$$\mathcal{U}(c) = \sum_{n=1}^{\infty} n\chi(n)\theta^n \sum_{v \in (\mathbb{Z}/c\mathbb{Z})^*} e\left(\tfrac{m\overline{v}+nv}{c}\right) = \sum_{v \in (\mathbb{Z}/c\mathbb{Z})^*} e(\tfrac{m\overline{v}}{c}) \sum_{n=1}^{\infty} n\chi(n)X^n. \quad (21)$$

Here and henceforth, we employ the standard shorthand $e(t) = e^{2\pi i t}$ and set $X = e(\frac{v}{c})\theta$. It follows that

$$|\mathcal{U}(c)| \le \sum_{v \in (\mathbb{Z}/c\mathbb{Z})^*} \left| \sum_{n=1}^{\infty} n\chi(n)X^n \right|.$$

This inner sum is

$$\sum_{n=1}^{\infty} n\chi(n)X^n = \sum_{\alpha=1}^{q} \chi(\alpha) \sum_{n \equiv \alpha(q)} nX^n$$

where

$$\sum_{n \equiv \alpha(q)} nX^n = \sum_{k=0}^{\infty} (\alpha + kq)X^{\alpha+kq} = \frac{\alpha X^{\alpha}}{1-X^q} + \frac{qX^{\alpha+q}}{(1-X^q)^2}\ .$$

Hence

$$\left| \sum_{n=1}^{\infty} n\chi(n)X^n \right| \le q\phi(q)(|1-X^q|^{-1} + |1-X^q|^{-2})$$

and thus

$$|\mathcal{U}(c)| \le q\phi(q) \sum_{v \in (\mathbb{Z}/c\mathbb{Z})^*} \left(|1-\theta^q e(\tfrac{vq}{c})|^{-1} + |1-\theta^q e(\tfrac{vq}{c})|^{-2}\right).$$

We write $\frac{qv}{c} = \frac{j}{c'}$ where $c' = c/\gcd(q,c)$ and $j \in (\mathbb{Z}/c'\mathbb{Z})^*$; for each fixed $j \in (\mathbb{Z}/c'\mathbb{Z})^*$ there are at most $\gcd(q,c)$ values of $v \in (\mathbb{Z}/c\mathbb{Z})^*$ such that $\frac{qv}{c} \equiv \frac{j}{c'} \bmod 1$. We thus obtain

$$\begin{aligned} |\mathcal{U}(c)| &\le q\phi(q)\gcd(q,c) \sum_{j \in (\mathbb{Z}/c'\mathbb{Z})^*} \left(|1-\theta^q e(\tfrac{j}{c'})|^{-1} + |1-\theta^q e(\tfrac{j}{c'})|^{-2}\right) \\ &\le 2q\phi(q)\gcd(q,c) \sum_{\substack{1 \le j \le \frac{c'}{2} \\ (j,c')=1}} \left(|1-\theta^q e(\tfrac{j}{c'})|^{-1} + |1-\theta^q e(\tfrac{j}{c'})|^{-2}\right), \end{aligned} \quad (22)$$

by pairing j and $c'-j$. From Lemma 8 of [9], we have $|1-e^z|^{-1} \le 2/|z|$ for z such that $|\operatorname{Im} z| \le \pi$ and $-2\pi/30 \le \operatorname{Re} z \le 0$, and hence

$$|\mathcal{U}(c)| \le 2q\phi(q)\gcd(q,c) \sum_{\substack{1 \le j < \frac{c'}{2} \\ (j,c')=1}} \left(\tfrac{c'}{\pi j} + \left(\tfrac{c'}{\pi j}\right)^2\right)\ .$$

It follows that

$$|\mathcal{U}(c)| \le 2q\phi(q)\gcd(q,c) \left(\frac{c'\log(\frac{ec'}{2})}{\pi} + \frac{(c')^2\zeta(2)}{\pi^2}\right) \le 2q\phi(q) \left(\frac{c\log(\frac{ec}{2})}{\pi} + \frac{c^2}{6}\right)$$

for $c \geq N \geq 400$. Therefore

$$|E_2'| \leq 32\pi^5 m^2 (2q\phi(q)) \sum_{N|c} c^{-4} \left(\frac{c \log(\frac{ec}{2})}{\pi} + \frac{c^2}{6} \right)$$
$$= 64q\phi(q)\pi^5 m^2 \left(\tfrac{\zeta(2)}{6} N^{-2} + \tfrac{1}{\pi}(\zeta(3)\log(\tfrac{eN}{2}) - \zeta'(3))N^{-3} \right),$$

again provided $N \geq 400$. Collecting estimates yields our result.

5. Proof of Proposition 10

To prove parts (i) and (ii) of Proposition 10, we begin by considering (12). Opening the Kloosterman sum as in (21), we obtain

$$\mathcal{S}(c) = \sum_{v \in (\mathbb{Z}/c\mathbb{Z})^*} e\left(\tfrac{m\overline{v}}{c}\right) \sum_{n=1}^{\infty} \chi(n)\theta^n e\left(\tfrac{nv}{c}\right) .$$

Setting as before $X = \theta e(\frac{v}{c})$, it follows that

$$\mathcal{S}(c) = \sum_{v \in (\mathbb{Z}/c\mathbb{Z})^*} e\left(\tfrac{m\overline{v}}{c}\right) \left(\frac{\sum_{\alpha=1}^{q} \chi(\alpha) X^\alpha}{(1 - X^q)} \right), \tag{23}$$

where $\overline{v} \in (\mathbb{Z}/c\mathbb{Z})^*$ is the multiplicative inverse of v. For part (i), we have $\chi(n) = (\frac{-4}{n})$ and thus

$$\frac{\sum_{\alpha=1}^{4} \chi(\alpha) X^\alpha}{1 - X^4} = \frac{X}{1 + X^2} .$$

Now we remark that for $n \in \mathbb{N}$,

$$|1 + X^n| = (1 + \theta^{2n} + 2\theta^n \cos\left(\tfrac{2\pi nv}{c}\right))^{\frac{1}{2}} = ((1 - \theta^n)^2 + 4\theta^n \cos^2(\tfrac{\pi nv}{c}))^{\frac{1}{2}} \tag{24}$$

via the identity $\cos(2u) = 2\cos^2(u) - 1$. It follows that

$$|\mathcal{S}(c)| \leq \sum_{v \in (\mathbb{Z}/c\mathbb{Z})^*} \left| \frac{X}{1 + X^2} \right| = \theta \sum_{v \in (\mathbb{Z}/c\mathbb{Z})^*} \left((1 - \theta^2)^2 + 4\theta^2 \cos^2\left(\tfrac{2\pi v}{c}\right)\right)^{-\frac{1}{2}}$$

whereby

$$|\mathcal{S}(c)| \leq \frac{1}{2} \sum_{v \in (\mathbb{Z}/c\mathbb{Z})^*} |\sec(\tfrac{2\pi v}{c})|.$$

We now write $\frac{2v}{c} = \frac{j}{c'}$ where $c' = \frac{c}{\gcd(2,c)}$ and $j \in (\mathbb{Z}/c'\mathbb{Z})^*$. Just as in the argument for bounding $\mathcal{U}(c)$, given before (22), we have

$$|\mathcal{S}(c)| \leq \frac{\gcd(2,c)}{2} \sum_{j \in (\mathbb{Z}/c'\mathbb{Z})^*} |\sec(\tfrac{\pi j}{c'})| \leq \gcd(2,c) \sum_{\substack{1 \leq j \leq \frac{c'}{2} \\ (j,c')=1}} \left|\sec(\tfrac{\pi j}{c'})\right|$$
$$\leq \gcd(2,c) \Big(\sum_{1 \leq j \leq M-1} \left|\sec(\tfrac{\pi j}{c'})\right| + \left|\sec(\tfrac{\pi M}{c'})\right| \Big),$$

where $M = \lfloor \frac{c'}{2} \rfloor$ and the last term only occurs if c' is odd. Note that we have the inequality

$$\phi(t) \leq \frac{1}{\delta} \int_{t - \frac{\delta}{2}}^{t + \frac{\delta}{2}} \phi(u)\, du \tag{25}$$

valid for convex functions. Applying this identity at the points $t = \frac{j}{c'}$ for $j = 1, \dots, M-1$ with $\delta = \frac{1}{c'}$ yields

$$|\mathcal{S}(c)| \le \gcd(2,c)\Big(c' \int_0^{\frac{M-1}{c'}+\frac{1}{2c'}} \sec(\pi t)\, dt + \sec\left(\pi\left(\tfrac{1}{2} - \tfrac{1}{2c'}\right)\right)\Big) \tag{26}$$

and since $\frac{M-1}{c'} + \frac{1}{2c'} \le \frac{1}{2} - \frac{1}{2c'}$, we have

$$\begin{aligned} |\mathcal{S}(c)| &\le c \int_0^{\frac{1}{2}-\frac{1}{2c'}} \sec(\pi t)\, dt + \gcd(2,c)\csc(\tfrac{\pi}{2c'}) \\ &= \frac{c}{\pi}\left(\log|\csc(\tfrac{\pi}{2c'}) + \cot(\tfrac{\pi}{2c'})| + \tfrac{\pi}{c'}\csc(\tfrac{\pi}{2c'})\right) \\ &= \frac{c}{\pi}\left(\log(c') + \log\left(\tfrac{1}{c'}|\csc(\tfrac{\pi}{2c'}) + \cot(\tfrac{\pi}{2c'})|\right) + \tfrac{\pi}{c'}\csc(\tfrac{\pi}{2c'})\right)\ . \end{aligned}$$

Noting that $c' \ge c/2 \ge 200$ and writing

$$c_0 = \max_{0 \le x \le \frac{1}{200}} \log(x|\csc(\tfrac{\pi x}{2}) + \cot(\tfrac{\pi x}{2})|) = \log(\tfrac{4}{\pi}) = 0.241564\dots$$

and

$$c_1 = \max_{0 \le x \le \frac{1}{100}} \pi x \csc\left(\tfrac{\pi x}{2}\right) = \tfrac{\pi}{100}\csc\left(\tfrac{\pi}{200}\right) = 2.000082\dots,$$

it follows that

$$|\mathcal{S}(c)| \le \frac{c}{\pi}\left(\log(c) + c_0 + c_1\right) \le \frac{c}{\pi}\left(\log(c) + 2.242\right),$$

as desired.

For part (ii), we have $\chi(n) = (\frac{-8}{n})$. Thus

$$\left|\frac{\sum_{\alpha=1}^{8}\chi(\alpha)X^\alpha}{1-X^8}\right| = \left|X\frac{1+X^2}{1+X^4}\right| = \theta\sqrt{\frac{1+\theta^4+2\theta^2\cos\left(\frac{4\pi v}{c}\right)}{(1-\theta^4)^2+4\theta^4\cos\left(\frac{4\pi v}{c}\right)}}$$

by (24). Hence

$$|\mathcal{S}(c)| \le \frac{\theta}{2\theta^2}\sum_{v\in(\mathbb{Z}/c\mathbb{Z})^*} |\sec\left(\tfrac{4\pi v}{c}\right)|\sqrt{1+\theta^4+2\theta^2\cos(\tfrac{4\pi v}{c})}\ .$$

As before, we write $\frac{4v}{c} = \frac{j}{c'}$ where $c' = \frac{c}{\gcd(4,c)}$, $j \in (\mathbb{Z}/c'\mathbb{Z})^*$, whence it follows that

$$|\mathcal{S}(c)| \le \frac{\gcd(4,c)}{2\theta}\sum_{j\in(\mathbb{Z}/c'\mathbb{Z})^*} |\sec\left(\tfrac{\pi j}{c'}\right)|\sqrt{1+\theta^4+2\theta^2\cos(\tfrac{\pi j}{c'})}\ .$$

Pairing j with $c'-j$, we have

$$|\mathcal{S}(c)| \le \frac{\gcd(4,c)}{2\theta}\sum_{\substack{1\le j\le \frac{c'}{2}\\(j,c')=1}} \sec\left(\tfrac{\pi j}{c'}\right)\phi(\cos(\tfrac{\pi j}{c'}))$$

where $\phi(t) = \sqrt{1+\theta^4+2\theta^2 t} + \sqrt{1+\theta^4-2\theta^2 t}$. Since $x = \sigma N\log N$, $\sigma \ge \frac{32}{\pi}$ and $N \ge 400$ we obtain the inequality $\theta \ge 0.9996$. It thus follows that

$$\phi(t) \le \phi^+(t) := \sqrt{2+2t} + \sqrt{2-2(0.9996)^2 t}$$

for $0 \le t \le 1$. Writing $M = \lfloor \frac{c'}{2} \rfloor$, we now have

$$|\mathcal{S}(c)| \le \frac{\gcd(4,c)}{2\theta}\Big(\sum_{1 \le j \le M-1} \sec\left(\tfrac{\pi j}{c}\right) \phi^+(\cos(\tfrac{\pi j}{c'})) + \sec(\ \tfrac{\pi M}{c'})\phi^+(\cos(\tfrac{\pi M}{c'}))\Big)$$

where the last term only occurs if c' is odd. As $\cos(\frac{\pi M}{c'}) = \sin(\frac{\pi}{2c'})$,

$$\sec(\tfrac{\pi M}{c'})\phi^+(\cos(\tfrac{\pi M}{c'})) \le \csc(\tfrac{\pi}{2c'})(\sqrt{2 + 2\sin(\tfrac{\pi}{200})} + \sqrt{2}) \le \frac{c'c_2}{\pi}$$

where

$$c_2 = c_1(\sqrt{2 + 2\sin(\tfrac{\pi}{200})} + \sqrt{2}) = 5.679214\ldots.$$

Note that here we have appealed to the inequality $c' \ge c/4 \ge 100$. Via calculus, we verify that $\sec(\pi t)\phi^+(\cos(\pi t))$ is convex on $[0, \frac{1}{2})$. Applying (25) in the same fashion as before,

$$|\mathcal{S}(c)| \le \frac{\gcd(4,c)}{2\theta}\Big(c' \int_0^{\frac{1}{2} - \frac{1}{2c'}} \sec(\pi t)\phi^+\left(\cos(\pi t)\right) dt + \frac{c'c_2}{\pi}\Big)\ .$$

It follows that

$$|\mathcal{S}(c)| \le \frac{c}{2\theta}\Big(\int_{0.4}^{\frac{1}{2} - \frac{1}{2c'}} \sec(\pi t)\phi^+\left(\cos(\pi t)\right) dt + c_3 + \frac{c_2}{\pi}\Big)$$

where

$$c_3 = \int_0^{0.4} \sec(\pi t)\phi^+(\cos(\pi t))\, dt = 1.496360\ldots\ .$$

By the variable change $t = 1/2 - t'$, we have

$$|\mathcal{S}(c)| \le \frac{c}{2\theta}\Big(\int_{\frac{1}{2c'}}^{0.1} \csc(\pi t')\phi^+\left(\sin(\pi t')\right) dt' + c_3 + \frac{c_2}{\pi}\Big)\ .$$

From the inequality $\phi^+(t) \le \sqrt{2}\,(2 + t/2)$, it follows that

$$|\mathcal{S}(c)| \le \frac{c}{2\theta}\Big(2\sqrt{2} \int_{\frac{1}{2c'}}^{0.1} \csc(\pi t')dt' + \tfrac{0.1}{\sqrt{2}} + c_3 + \frac{c_2}{\pi}\Big)\ .$$

The integral here may be evaluated as

$$\begin{aligned}\int_{\frac{1}{2c'}}^{0.1} \csc(\pi t')dt' &= \frac{1}{\pi}\log\left|\csc\left(\tfrac{\pi}{2c'}\right) + \cot\left(\tfrac{\pi}{2c'}\right)\right| - \frac{c_4}{\pi} \\ &= \frac{\log c'}{\pi} + \frac{1}{\pi}\log\left(\tfrac{1}{c'}\left|\csc\left(\tfrac{\pi}{2c'}\right) + \cot\left(\tfrac{\pi}{2c'}\right)\right|\right) - \frac{c_4}{\pi}\end{aligned}$$

where $c_4 = \log|\csc(0.1\pi) + \cot(0.1\pi)| = 1.842730\ldots$. Defining

$$c_5 = \max_{0 \le x \le \frac{1}{100}} \log(x|\csc(0.5\pi x) + \cot(0.5\pi x)|) = \log(\tfrac{4}{\pi}) = 0.241564\ldots$$

and noting the inequality $c' \ge \frac{c}{4} \ge 100$, we have

$$\int_{\frac{1}{2c_1}}^{0.1} \csc(\pi t')\, dt' \le \frac{1}{\pi}\left(\log(c') + (c_5 - c_4)\right),$$

and hence deduce that

$$\begin{aligned}\mathcal{S}(c) &\leq \frac{c}{\pi}\left(\frac{\sqrt{2}\log(c')}{\theta} + \frac{1}{0.9996}\left(\sqrt{2}(c_5-c_4) + \pi(\tfrac{0.1}{2\sqrt{2}} + 0.5c_3) + 0.5c_2\right)\right) \\ &\leq \frac{c}{\pi}\left(\frac{\sqrt{2}\log(c)}{\theta} + 3.038\right),\end{aligned}$$

as claimed.

We now turn our attention to the proof of part (iii) of Proposition 10. We write $c = p^\alpha b$ with $\gcd(p,b) = 1$. If we suppose that $p \mid n$, then, via Lemme 2.10 of [15], we may conclude that $S(1,n;c) = 0$. We may therefore assume that $\gcd(n,p) = 1$. By the twisted multiplicativity of the Kloosterman sum,

$$S(1,n;c) = S(\overline{p^\alpha}, \overline{p^\alpha}n; b)S(\overline{b}, \overline{b}n; p^\alpha)\ .$$

The Kloosterman sum with modulus p^α may be evaluated in an elementary fashion. In particular, we have $S(\overline{b}, \overline{b}n; p^\alpha) = 0$ unless n is congruent to a square modulo p^α (see pages 16–18 of Salié [16] for an explanation). Supposing that $n \equiv l^2 \pmod{p^\alpha}$, we have that

$$|S(\overline{b}, \overline{b}l^2; p^\alpha)| = |S(l\overline{b}, l\overline{b}; p^\alpha)| \leq 2p^{\frac{\alpha}{2}}$$

by Lemmata 4.1 and 4.2 of [14]. Consequently, $|S(1,n;c)| \leq 2d(b)\sqrt{c}$ if $\left(\frac{n}{p}\right) = 1$ (and otherwise it vanishes). In addition, since χ by supposition is a character of even conductor, it is only supported on odd integers. We deduce that if $c = p^\alpha b$ with $\gcd(b,p) = 1$ then

$$|\mathcal{S}(c)| \leq d(b)c^{\frac{1}{2}} \sum_{\substack{n \text{ odd} \geq 1 \\ (n,p)=1}} \left(1 + \left(\frac{n}{p}\right)\right) e^{-2\pi n/x} = d(b)c^{\frac{1}{2}} g(\theta)$$

where $g(\theta) = \sum_{\substack{n \text{ odd} \geq 1 \\ (n,p)=1}} \left(1 + \left(\frac{n}{p}\right)\right)\theta^n$. If we set $a_n = \left(1 + \left(\frac{n}{p}\right)\right)\theta^n$, we obtain the identity

$$g(\theta) = \sum_{\substack{n \text{ odd} \geq 1 \\ (n,p)=1}} a_n = \sum_{n \geq 1}(a_n - a_{2n} - a_{pn} + a_{2pn})\ .$$

Note that if $p \mid k$ then

$$\sum_{n \geq 1} a_{kn} = \sum_{n=1}^{\infty} \theta^{kn} = \frac{\theta^k}{1-\theta^k}$$

and if $(p,k) = 1$ then

$$\sum_{n \geq 1} a_{kn} = \sum_{n=1}^{\infty} \theta^{kn} + \sum_{a=1}^{p-1}\left(\frac{kn}{p}\right) \sum_{\substack{n \geq 1 \\ n \equiv a(p)}} \theta^{kn} = \frac{\theta^k}{1-\theta^k} + \frac{\sum_{a=1}^{p-1}\left(\frac{ka}{p}\right)\theta^{ak}}{1-\theta^{kp}}\ .$$

Combining these last two formulae with our expression for $g(\theta)$ yields

$$\begin{aligned} & g(\theta) \\ &= \Big(\frac{\theta}{1-\theta} + \frac{\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\theta^a}{1-\theta^p}\Big) - \Big(\frac{\theta^2}{1-\theta^2} + \frac{\sum_{a=1}^{p-1}\left(\frac{2a}{p}\right)\theta^{2a}}{1-\theta^{2p}}\Big) - \frac{\theta^p}{1-\theta^p} + \frac{\theta^{2p}}{1-\theta^{2p}} \\ &= \frac{\theta}{1-\theta^2} - \frac{\theta^p}{1-\theta^{2p}} + \frac{\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\theta^a}{1-\theta^p} - \frac{\sum_{a=1}^{p-1}\left(\frac{2a}{p}\right)\theta^{2a}}{1-\theta^{2p}} \ . \end{aligned}$$

Thus we deduce that

$$|\mathcal{S}(c)| \le d(b)c^{1/2}g(\theta) = \frac{d(c)}{d(p^\alpha)}c^{1/2}g(\theta) \le \frac{1}{3}d(c)c^{1/2}g(\theta)$$

since $\alpha \ge 2$.

6. Proof of Lemma 12

We will now finish the proof of Lemma 14 by proving Lemma 12. Since

$$d(n) \le 2\sum_{k|n,k\le\sqrt{n}} 1,$$

the sum we wish to estimate is bounded above by

$$\begin{aligned} & 2\sum_{k=1}^{\infty} k^{-\frac{3}{2}} \sum_{l\ge \max k,\frac{u}{k}} l^{-\frac{3}{2}} \le 2\left(\sum_{k\le\sqrt{u}} k^{-3/2}\sum_{l\ge\frac{u}{k}} l^{-3/2} + \sum_{k\ge\sqrt{u}} k^{-3/2}\sum_{l\ge k} l^{-3/2}\right) \\ & \le 2\left(\sum_{k\le\sqrt{u}} k^{-3/2}\left(2\,(u/k)^{-1/2} + (u/k)^{-3/2}\right) + \sum_{k\ge\sqrt{u}} k^{-3/2}(2k^{-1/2}+k^{-3/2})\right) \ . \end{aligned}$$

The first sum within the brackets of this last expression is

$$\begin{aligned} \frac{2}{\sqrt{u}}\sum_{k\le\sqrt{u}} k^{-1} + \frac{1}{u} &\le \frac{2}{\sqrt{u}}\left(\log(\sqrt{u}) + \gamma + \frac{7}{12\sqrt{u}}\right) + \frac{1}{u} \\ &\le \frac{\log u + 2\gamma}{\sqrt{u}} + \frac{13}{6u}, \end{aligned}$$

while the second sum within the brackets is

$$\le 2\sum_{k\ge\sqrt{u}} k^{-2} + \sum_{k\ge\sqrt{u}} k^{-3} \le \frac{2}{\sqrt{u}-1} + \frac{1}{2(\sqrt{u}-1)^2} \ .$$

Collecting estimates thus yields

$$h(u) := \sum_{n>u}\frac{d(n)}{n^{3/2}} \le \frac{2\log u + 4\gamma}{\sqrt{u}} + \frac{4}{\sqrt{u}-1} + \frac{13}{3u} + \frac{1}{(\sqrt{u}-1)^2} \ .$$

It follows that

$$h(u) \le \frac{2\log u + 4\gamma + 4 + \epsilon}{\sqrt{u}}$$

for $u \ge 60000$, where

$$\epsilon = \max_{u\ge 60000} \sqrt{u}\Big(\frac{4}{\sqrt{u}(\sqrt{u}-1)} + \frac{13}{3u} + \frac{1}{(\sqrt{u}-1)^2}\Big) \le 0.04.$$

We thus deduce Lemma 12.

7. Modular forms tables

We will now complete the proof of Proposition 6. From Lemma 14 and the discussion at the start of Section 3, it remains to exhibit weight 2 cuspforms f at level p^2 or $2p^2$ satisfying the criteria of Proposition 5, where

$$p \in \{11, 13, 19, 23, 29, 31, 37, 43, 53, 59\}, \quad \text{if } \chi = \chi_{-4},$$

and

$$p \in \{7, 11, 13, 19, 23, 29, 31, 37, 43, 53, 59, 61, 67, 79, 83\}, \quad \text{if } \chi = \chi_{-8}.$$

For many of the values of p under consideration, it suffices to consider forms of dimension 1, i.e. those corresponding to elliptic curves over $\mathbb{Q}$. Indeed, a short Pari computation implies that we may take, using Cremona's notation for the corresponding curve, our forms f as follows

p	f	p	f	p	f
11	$121b$	37	$2738c$	67	$4489a$
13	$338b$	43	$1849a$	79	$12482e$
19	$722d$	53	$2809a$	83	$13778b$
29	$1682g$	59	$6962i$		
31	$1922c$	61	$3721a$		

For $11 \leq p \leq 59$, these forms have the desired nonvanishing of their twisted L-functions, for twists by either character χ_{-4} or χ_{-8}. For $p \geq 61$, they have this property for χ_{-8}. With this in mind, it remains to handle $p \in \{7, 23, 47\}$ for character χ_{-4}, and $p \in \{23, 47, 71\}$ for χ_{-8}; we necessarily restrict our attention to higher dimensional forms. For these primes, a rather lengthy Magma computation confirms that we may choose forms f as follows (in Stein's notation) :

p	χ	f	p	χ	f
7	χ_{-4}	98(2)	47	χ_{-4}	2209(9)
23	χ_{-4}	529(7)	47	χ_{-8}	2209(9)
23	χ_{-8}	529(7)	71	χ_{-8}	5041(4)

These computations finish the proof of Proposition 6. A detailed Magma script for the calculations described here is available at

http://www.math.ubc.ca/∼bennett/BeElNg

We are left, therefore, to prove Proposition 7.

8. Proof of Proposition 7 : easy cases

Let us begin by noting that equation (5) has been shown by Bruin to have no solutions in coprime positive integers for $n = 5$ and $n = 6$, in [3] and [4], respectively. Furthermore, the cases with $n = 4$ are relatively classical. The change of variables

$$Y = \frac{4C}{A^3}\left(B - C^2\right), \quad X = -\frac{2}{A^2}\left(B + C^2\right)$$

takes a positive solution to (5) , with $n = 4$, to the curve $Y^2 = X^3 + 4X$, Cremona's 32a1. This curve has Mordell-Weil rank 0 over $\mathbb{Q}$ and full 2-torsion, whereby all its rational points have $Y = 0$; these correspond to solutions to (5) with $ABC = 0$. Similarly solutions to (6) with $n = 4$ correspond to rational points on an elliptic curve over $\mathbb{Q}$ of conductor 64 and rank 0; again only trivial solutions accrue.

To complete our analysis of (5) and (6), we will consider the first of these equations with $n = 9$, and the second for $n \in \{5, 6, 7, 9\}$. In the first case, factoring over $\mathbb{Q}(\sqrt{-1})$, we have

$$A^2 + B\sqrt{-1} = (a + b\sqrt{-1})^9,$$

for coprime nonzero integers a and b of opposite parity, whence

$$A^2 = a(a^2 - 3b^2)(a^6 - 33a^4b^2 + 27a^2b^4 - 3b^6).$$

It follows that

$$a^6 - 33a^4b^2 + 27a^2b^4 - 3b^6 = \epsilon z^2,$$

for z a positive integer and $\epsilon \in \{\pm 1, \pm 3\}$. By consideration of the reduction of this equation modulo 8, we see that either $\epsilon = 1$ or $\epsilon = -3$. In the first instance, since the elliptic curve given by

$$Y^2 = X^3 - 33X^2 + 27X - 3,$$

of conductor 1296, is readily shown to have no finite rational points, there are no solutions. In the second, writing $a = 3c$, we have that

$$z^2 = b^6 - 81b^4c^2 + 891b^2c^4 - 243c^6,$$

and the fact that the curve

$$Y^2 = X^3 - 81X^2 + 891X - 243$$

has rank 0 over $\mathbb{Q}$ and trivial torsion leads to the desired contradiction.

It remains to treat equation (6) with $n \in \{5, 6, 7, 9\}$. Factoring over $\mathbb{Q}(\sqrt{-2})$, we have

$$A^2 + B\sqrt{-2} = \pm(a + b\sqrt{-2})^n,$$

for a and b coprime nonzero integers (if n is odd, we may assume further that the sign is a positive one). We will handle the two composite values of n first. If $n = 6$, we find that

$$A^2 = \pm(a^6 - 30a^4b^2 + 60a^2b^4 - 8b^6) = \pm(a^2 - 2b^2)(a^4 - 28a^2b^2 + 4b^4)$$

Since a and b are coprime, it is easy to show that the two factors on the right hand side here are also coprime, so that there exists an integer z such that

$$\pm z^2 = a^4 - 28a^2b^2 + 4b^4.$$

Reducing mod 4, we see that the sign on the left hand side must be positive.

Writing

$$Y = \frac{4a}{b^3}\left(z - a^2 + 14b^2\right), \quad X = \frac{-2}{b^2}\left(z - a^2 + 14b^2\right)$$

we obtain

$$Y^2 = X^3 + 56X + 768X.$$

This curve (of conductor 192) has rank 0 and full 2-torsion over $\mathbb{Q}$. The torsion points (with $Y = 0$) map back to a point on our original curve with $b = y = 0$. Similarly, if $n = 9$, we may, without loss of generality, write

$$A^2 = a^9 - 72a^7b^2 + 504a^5b^4 - 672a^3b^6 + 144ab^8$$

The form on the right hand side of this equation factors as

$$a(a^2 - 6b^2)(a^6 - 66a^4b^2 + 108a^2b^4 - 24b^6).$$

If 3 fails to divide a, then this last form is coprime to the others. By considering both sides modulo 8, we see that there exists an integer z such that

$$z^2 = a^6 - 66a^4b^2 + 108a^2b^4 - 24b^6.$$

This is a double cover of the curve

$$Y^2 = X^3 - 66X^2 + 108X - 24$$

which is Cremona's 5184ba, with trivial Mordell-Weil group over $\mathbb{Q}$. If $3 \mid a$, then, again after consdering the reduction mod 8, we have

$$a^6 - 66a^4b^2 + 108a^2b^4 - 24b^6 = 3z^2$$

for some integer z. Writing $Y = 27z/a^3$ and $X = -18b^2/a^2$, we thus have

$$Y^2 = X^3 + 81X^2 + 891X + 243.$$

This is Cremona's 1296f, again with trivial $E/\mathbb{Q}$.

9. Proof of Proposition 7 : hard cases

It remains only to treat (6) with $n = 5$ and $n = 7$. These equations, as far as we can see, require more than routine arguments involving rank 0 elliptic curves over $\mathbb{Q}$. To replace these, we turn to modern Chabauty-type arguments, mostly now implemented in Magma. A useful reference for what we have in mind are the papers of Bruin [4], and Bruin and Flynn [5]. A more detailed description of the work in [4] is available in [2].

In the case $n = 5$, we may write

$$A^2 = a^5 - 20a^3b^2 + 20ab^4 = a\left(a^4 - 20a^2b^2 + 20b^4\right), \tag{27}$$

for coprime a and b. We prove

Proposition 15. *The only solutions to equation (27) in coprime integers a and b, and integer A are with*

$$(a, b) \in \{(0, \pm 1), (1, 0), (1, \pm 1)\}.$$

Only the solutions $(a, b) = (1, \pm 1)$ are relevant to our original problem; they lead to the identity $1^4 + 2 \cdot 11^2 = 3^5$.

Let us define β by $\beta^4 - 10\beta^2 + 20 = 0$, so that the field $\mathbb{Q}(\beta)$ is Galois with integral basis $1, \beta, \beta^2/2, \beta^3/2$, ring of integers $\mathcal{O}_{\mathbb{Q}(\beta)}$ and units

$$\mathcal{O}^*_{\mathbb{Q}(\beta)} =< -1, 2 - \beta^2/2, 3 + 2\beta - \beta^2 - \beta^3/2, 7 + 4\beta - \beta^2 - \beta^3/2 > .$$

We may factor $X^4 - 20X^2 + 20$ as

$$\left(X - \frac{1}{2}\left(\beta^3 - 4\beta\right)\right)\left(X + \frac{1}{2}\left(\beta^3 - 4\beta\right)\right)\left(X - \frac{1}{2}\left(\beta^3 - 8\beta\right)\right)\left(X + \frac{1}{2}\left(\beta^3 - 8\beta\right)\right).$$

Choosing $\alpha = \frac{1}{2}\left(\beta^3 - 4\beta\right)$ (so that $\alpha^4 - 20\alpha^2 + 20 = 0$), we find that

$$a = \mathrm{Norm}(\delta)a_4^2 \text{ and } a - \alpha b = \delta\left(a_0 + a_1\beta + \frac{a_2}{2}\beta^2 + \frac{a_3}{2}\beta^3\right)^2,$$

where, in the notation of [4], $\delta \in L(S,2)$ for $S = \{2,5\}$ and $L = \mathbb{Q}$ or $\mathbb{Q}(\beta)$, and the a_i are rational integers. Additionally,

$$(a/b)^4 - 20(a/b)^2 + 20 = \mathrm{Norm}(\delta)\left(A/(a_4b^2)\right)^2,$$

whereby local analysis at 2 and 5 guarantees that we may assume $\mathrm{Norm}(\delta) = 1, 5$ or 20. The primes dividing 2 and 5 in $\mathcal{O}$, say $-\beta^2 - \beta + 4$ and $\beta^3/2 + \beta^2/2 - 2\beta$, have norms -4 and -5, respectively. Since all the units in $\mathcal{O}$ have positive norm, it follows that we may assume that δ is either a squarefree unit or has norm 20; local arguments using primes up to $p = 31$ (as described in some detail in [2]), in fact enable us to restrict attention to the following values of $\pm\delta$:

$$1, \frac{1}{8}(\alpha^3 + \alpha^2 - 22\alpha - 22), \frac{1}{4}(5\alpha^3 + 22\alpha^2 - 2\alpha - 20), \frac{1}{8}(65\alpha^3 + 296\alpha^2 + 2\alpha - 240).$$

For each of these δ, we are thus led to an elliptic curve of the shape

$$E_\delta \ : \ \frac{\mathrm{Norm}(\delta)}{\delta}Y^2 = X^4 + \frac{1}{2}(\beta^3 - 4\beta)X^3 + (4\beta^2 - 30)X^2 + (-3\beta^3 + 20\beta)X.$$

Here, $X = a/b$ and $Y \in \mathbb{Q}(\beta)$. We now employ Magma to determine the Mordell-Weil groups of these curves (over $\mathbb{Q}(\beta)$) up to finite index, via a 2-isogeny-descent. On each case, we encounter a rank less than 3, whence we might hope that a Chabauty-type argument may prove feasible. In every case, as it transpires, a prime $p \leq 31$ yields the desired result; only the values $X = 0, \pm 1$ and ∞ occur, as claimed. A detailed Magma script for these computations is available, again at

http://www.math.ubc.ca/∼bennett/BeElNg

We take this opportunity to express thanks to Nils Bruin for carrying out many of the computations described here, and, in particular, for the use of his specialty Magma routine "TwoCoverDescent".

Lastly, let us suppose that $n = 7$ in equation (6), whereby we may write

$$A^2 = a\left(a^6 - 42a^4b^2 + 140a^2b^4 - 56b^6\right).$$

Arguing modulo 8, we thus have that

$$a^6 - 42a^4b^2 + 140a^2b^4 - 56b^6 = \delta z^2$$

for $\delta \in \{-7, 1\}$ and z a positive integer. If $\delta = -7$, then, writing $a = 7c$,

$$8b^6 - 980b^4c^2 + 14406b^2c^4 - 16807c^6 = z^2.$$

Since the curve

$$Y^2 = X^3 - 245X^2 + 7203X - 16807$$

(Cremona's 392b) has rank 0 and trivial torsion over $\mathbb{Q}$, there are thus no solutions with $\delta = -7$. In the case $\delta = 1$, we are led to consider the curve

$$C \ : \ Y^2 = X^6 - 42X^4 + 140X^2 - 56.$$

Here, from Magma, we have that the Mordell-Weil rank of the Jacobian of C is 2, ensuring that a direct Chabauty-type argument will not suffice to determine the rational points on C. We note also that the evident genus 1 quotient $Y^2 = x^3 - 42x^2 + 140x - 56$ has positive rank, so it also fails to supply an easy way out.

We argue as in [13]. Let us define $K = \mathbb{Q}(\theta)$ where $\theta^3 - 42\theta^2 + 140\theta - 56 = 0$. It follows that $\mathcal{O}_K$ has an integral basis given by

$$1,\ \frac{1}{8}\theta + \frac{1}{4},\ \frac{1}{64}\theta^2 + \frac{1}{16}\theta + \frac{1}{16},$$

class number 1, discriminant 49 and

$$\mathcal{O}_K^* =< -1, \theta^2/64 - 9\theta/16 - 3/16, \theta^2/64 - 11\theta/16 + 25/16 > .$$

We have, for (X, Y) on C,

$$Y^2 = (X^2 - \theta)(X^4 - (\theta - 42)X^2 + (\theta^2 - 42\theta + 140)),$$

and

$$X^4 - (\theta - 42)X^2 + (\theta^2 - 42\theta + 140) = \delta Y_1^2$$

where $\delta, Y_1 \in \mathbb{Q}(\theta)$. As in the preceding example, local considerations show that most of the δ-twists may be discounted; in this case only $\delta = 1$ survives our local sieve. Choosing a point on this curve, say

$$\left(0 : \frac{1}{16}(\theta^2 - 44\theta + 196) : 1\right),$$

we may convert this to Weierstrass form :

$$E\ :\ y^2 = x^3 + \frac{1}{1792}\left(3\theta^2 - 11\theta + 6\right)x^2 + \frac{1}{401408}\left(207\theta^2 - 747\theta + 302\right)x.$$

A full 2-descent now shows that E/K has rank 1 whence, after finding a generator, a Chabauty-type argument at $p = 5$ shows that the only K-rational points on E with $\mathbb{Q}$-rational x-coordinate correspond to $x = 0, \infty$. Only the latter correspond to (the known) rational points on C. Once more, a detailed Magma script for these computations is available at

http://www.math.ubc.ca/∼bennett/BeElNg

This completes the proof of Proposition 7 and hence of Theorem 1.

Acknowledgements. The authors would like to thank N. Bruin, K. Soundararajan and S. Yazdani numerous helpful discussions and invaluable computational assistance.

References

[1] Michael A. Bennett and Maurice Mignotte. Integral points on congruent number curves, in preparation.
[2] Nils Bruin. Chabauty methods and covering techniques applied to generalised Fermat equations, PhD-thesis, University of Leiden, 1999.
[3] Nils Bruin. The diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$, Compositio Math. 118 (1999), 305–321.
[4] Nils Bruin. Chabauty methods using elliptic curves, J. Reine Angew. Math. 562 (2003), 27–49.
[5] Nils Bruin and E. Victor Flynn. Towers of 2-covers of hyperelliptic curves, Trans. Amer. Math. Soc. 357 (2005), 4329–4347.
[6] Henri Darmon and Andrew Granville. On the equations $x^p + y^q = z^r$ and $z^m = f(x, y)$, Bull. London Math. Soc. 27 (1995), 513–544.
[7] Luis Dieulefait and Jorge Jimémez Urroz. Solving Fermat-type equations $x^4 + dy^2 = z^p$ via modular Q-curves over polyquadratic fields, Preprint, available as arXiv math.NT/0611663.
[8] William Duke, The critical order of vanishing of automorphic L-functions with large level, Invent. Math. 119 (1995), 165–174.

[9] Jordan S. Ellenberg, On the error term in Duke's estimate for the average special value of L-functions, Canad. Math. Bull. 48 (2005), 535–546.
[10] Jordan S. Ellenberg. Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$. Amer. J. Math. 126 (2004), 763–787.
[11] Jordan S. Ellenberg. **Q**-curves and Galois representations, in *Modular Curves and Abelian Varieties*, J. Cremona, J.C. Lario, J. Quer and K. Ribet, eds. (Birkhaäuser, 2004)
[12] Noam Elkies. http://modular.fas.harvard.edu/Tables/nature/
[13] E. Victor Flynn and Joseph Wetherell. Finding rational points on bielliptic genus 2 curves, Manuscripta Math.100 (1999), 519–533.
[14] Henryk Iwaniec, *Topics in classical automorphic forms*, Graduate Studies in Math. **17**, Providence, RI (1997).
[15] Emmauel Royer, Petits zéros de fonctions L de formes modulaires, Acta Arith. XCIX.2 (2001), 147–172.
[16] Hans Salié, Über die Kloostermanschen Summen $S(u, v; q)$, Math. Z., 34 (1931), 91–109.
[17] Jean-Pierre Serre, Sur les répresentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987), 179–230.