PERFECT POWERS EXPRESSIBLE AS SUMS OF TWO CUBES

IMIN CHEN AND SAMIR SIKSEK

To John Cannon and Derek Holt

ABSTRACT. Let $n \geq 3$. This paper is concerned with the equation $a^3 + b^3 = c^n$, which we attack using a combination of the modular approach (via Frey curves and Galois representations) with obstructions to the solutions that are of Brauer–Manin type. We shall show that there are no solutions in coprime, non-zero integers a, b, c, for a set of *prime* exponents n having Dirichlet density $\frac{28219}{44928} \approx 0.628$, and for a set of exponents n having natural density 1.

1. INTRODUCTION

Let p, q, $r \in \mathbb{Z}_{\geq 2}$. The equation

$$a^p + b^q = c^r \tag{1}$$

is known as the Fermat–Catalan equation with signature (p, q, r). As in Fermat's Last Theorem, one is interested in integer solutions a, b, c. Such a solution is called *non-trivial* if $abc \neq 0$, and *primitive* if a, b, c are coprime. Let $\chi = p^{-1} + q^{-1} + r^{-1}$. The parametrization of non-trivial primitive solutions for (p, q, r) with $\chi \geq 1$ has now been completed ([5], [19]). The Generalized Fermat Conjecture [15], [17] is concerned with the case $\chi < 1$. It states that the only non-trivial primitive solutions to (1) with $\chi < 1$ are

$$1 + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 17^7 + 76271^3 = 21063928^2, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 43^8 + 96222^3 = 30042907^2, \quad 33^8 + 1549034^2 = 15613^3.$$

The Generalized Fermat Conjecture has been established for many signatures (p, q, r), including for several infinite families of signatures: Fermat's Last Theorem (p, p, p) by Wiles and Taylor [31], [30]; $(p, p, 2)$ and $(p, p, 3)$ by Darmon and Merel [18]; $(2, 4, p)$ by Ellenberg [20] and Bennett, Ellenberg and Ng [3]; $(2p, 2p, 5)$ by Bennett [2]. For an exhaustive survey see [5]. An older but still very useful survey is [24]. All these infinite cases have been established through the same steps as Wiles' proof of Fermat's Last Theorem, or some strengthening of this approach. We call this approach via the modularity of Galois representations of elliptic curves and Ribet's Level-Lowering Theorem, the modular approach. In [16], Darmon suggests that

Date: February 12, 2009.

2000 *Mathematics Subject Classification.* Primary 11D41, Secondary 11G30.

Key words and phrases. Diophantine equations, Frey curves, level-lowering, Brauer–Manin obstruction.

I. Chen is supported by an NSERC Discovery Grant. S. Siksek is supported by a grant from the UK Engineering and Physical Sciences Research Council, and by a Marie–Curie International Reintegration Grant (MIRG-CT-2006-044530).

the Generalized Fermat Conjecture might be approached through a highly ambitious extension of the modular approach where Hilbert modular forms and certain abelian varieties of higher dimension respectively play the rôle of elliptic modular forms and elliptic curves. However, for now it seems that the way forward is to combine the modular approach with other techniques, as in the beautiful paper of Poonen, Schaefer and Stoll [26] where they solve equation (1) with signature $(2, 3, 7)$.

In this paper we shall be concerned with the following special case of the Generalized Fermat Conjecture.

Conjecture. *Let $n \geq 3$. The equation*

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

does not have any non-trivial primitive solutions.

We shall attack the conjecture (with only partial success) using a combination of the modular approach, together with an obstruction to solutions that is of the Brauer–Manin type.

Equation (2) has been studied by Kraus [23], Bruin [10] and Dahmen [14]. Indeed, Kraus studies this equation using Frey curves and Galois representations and deduces a practical criterion for proving the conjecture for a particular prime exponent $n \geq 17$. Kraus also used a computer program to check his criterion for prime exponents $17 \leq n < 10^4$. Bruin [10] proved the conjecture for $n = 4$, 5, using descent and Chabauty. Dahmen [14, Section 3.3.2] strengthens Kraus' argument to prove the conjecture for $n = 5$, 7, 11, 13. Of course, for $n = 3$, the result is classical (a special case of Fermat's Last Theorem). Thus combined, the results of Kraus, Bruin and Dahmen show that equation (2) does not have non-trivial primitive solutions for $3 \leq n \leq 10^4$.

In this paper we prove the following theorem.

Theorem 1. *Let $n \geq 3$. Suppose n is divisible by some positive integer d satisfying* **any** *of the following congruences,*

(I) $d \equiv 2,\ 3 \pmod 5$,
(II) $d \equiv 17,\ 61 \pmod{78}$,
(III) $d \equiv 51,\ 103,\ 105 \pmod{106}$,
(IV) $d \equiv 43,\ 49,\ 61,\ 79,\ 97,\ 151,\ 157,\ 169,\ 187,\ 205,\ 259,\ 265,\ 277,\ 295,\ 313,\ 367,\ 373,\ 385,\ 403,\ 421,\ 475,\ 481,\ 493,\ 511,\ 529,\ 583,\ 589,\ 601,\ 619,\ 637,\ 691,\ 697,\ 709,\ 727,\ 745,\ 799,\ 805,\ 817,\ 835,\ 853,\ 907,\ 913,\ 925,\ 943,\ 961,\ 1015,\ 1021,\ 1033,\ 1051,\ 1069,\ 1123,\ 1129,\ 1141,\ 1159,\ 1177,\ 1231,\ 1237,\ 1249,\ 1267,\ 1285 \pmod{1296}$.

Then equation (2) *has no non-trivial primitive solutions.*

We will show (Section 10) that the set of *prime* exponents n that satisfy the conditions of the theorem has Dirichlet density $\frac{28219}{44928} \approx 0.628$. However, as we also show in Section 10, the set of positive integers n satisfying the conditions of the theorem has natural density 1.

The proof of Theorem 1 relies in part on Kraus' earlier work. Roughly speaking, for any prime $\ell \neq 2$, 3, Kraus' method gives congruences modulo ℓ for unknowns a, b in (2). The proof also uses ideas from the work of Bright and Siksek [8]. Indeed we shall show how the non-trivial primitive solutions to (2) give rise to rational

points on the hyperelliptic curve

$$\delta^2 + \frac{1}{27} = 4\epsilon^n. \tag{3}$$

For odd exponent n, the function $f = \epsilon - 1$ on this hyperelliptic curve has a divisor which is a norm [1] from the quadratic extension $\mathbb{Q}(\sqrt{321})$. In [8] (see also [28]) it is shown how a function on a curve whose divisor is a norm from an abelian extension can give rise to an obstruction to weak approximation (that is of Brauer–Manin type). In layman's terms, this merely means that we obtain congruence restrictions on the rational points of the curve. The congruence restrictions are obtained through an application of the Law of Quadratic Reciprocity. Combining these congruence restrictions with with the congruences for a, b obtained via Kraus' modular approach shows that equation (2) has no non-trivial primitive solutions if the exponent n is divisible by some positive integer $d \equiv 51,\ 103,\ 105 \pmod{106}$. This a part of Theorem 1.

To obtain the remaining results of Theorem 1 we need to consider two other hyperelliptic curves associated to (2) defined over $\mathbb{K} = \mathbb{Q}(\omega)$ where ω is a primitive cube root of 1. The functions we employ are defined over $\mathbb{Q}(\zeta)$ and $\mathbb{K}(\zeta)$ for various roots of unity ζ, and we employ the Law of Quadratic Reciprocity over number fields. Again the congruences obtained here are combined with the congruences from the modular approach and this is used to deduce the remainder of Theorem 1.

Whilst [8] is an important motivation in our proof of Theorem 1, we shall not require the high-brow machinery involved in that paper, and will need nothing more than the Law of Quadratic Reciprocity over number fields. The use of quadratic reciprocity is in the spirit of the less conceptual, but more concrete, earlier paper [27], which uses quadratic reciprocity to obtain congruence restrictions for solutions of hyperelliptic curves.

We shall also give a refinement of Kraus' criterion for the non-existence of non-trivial primitive solutions for a given prime exponent n. We shall use our refined criterion to prove the following.

Theorem 2. *Equation* (2) *has no solutions for exponents* $3 \le n \le 10^9$.

All computations in this paper were performed using the computer packages `MAGMA` [7] and `pari/gp` [1].

We would like to thank the referee for his careful reading of the paper and for pointing out several corrections.

2. Kraus' Modular Approach

In this section we summarise what we need from Kraus' paper [23]. For a basic tutorial on the modular approach, see [13, Chapter 15] or [29]. For a somewhat more conceptual introduction, we recommend Sander Dahmen's recent Ph.D. thesis [14].

Let $n \ge 17$ be prime and let (a, b, c) be a non-trivial primitive solution to equation (2). Kraus associates the solution (a, b, c) to the Frey curve

$$E_{a,b}:\ Y^2 = X^3 + 3abX + b^3 - a^3, \tag{4}$$

[1] For odd n, the function $f = \epsilon - 1$ has divisor $P + P' - 2\infty$ where $P = (1, \sqrt{321}/9)$ and $P' = (1, -\sqrt{321}/9)$. In other words, the divisor of f is the norm (or trace) of the divisor $P - \infty$ which is defined over $\mathbb{Q}(\sqrt{321})$.

and studies the Galois representation on its n-torsion

$$\varrho_{a,b} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E_{a,b}[n]).$$

Kraus uses results of Mazur to show that this representation is irreducible. He shows that the Serre weight is 2, and computes the Serre conductor $N_{a,b}$, which depends on various modulo 2 and modulo 3 congruence conditions on the triple (a, b, c). Next, Ribet's Level-Lowering Theorem is invoked to show that $\varrho_{a,b}$ arises from a cuspidal newform of weight 2 and level $N_{a,b}$. For all but one of the possible values of the Serre conductor $N_{a,b}$, Kraus obtains a contradiction, either by using a deep result of Darmon and Merel [18], or by a careful study of size of the image of the inertia subgroup at 3 under $\varrho_{a,b}$. The exceptional value of $N_{a,b}$ is 72, and the exceptional newform that has not yet been eliminated corresponds to the elliptic curve

$$E : \ Y^2 = X^3 + 6X - 7, \tag{5}$$

of conductor 72 (this curve is $72A$ in the Antwerp tables [6], and curve $72A1$ in Cremona's tables [12]). The following proposition collects some facts from Kraus' paper.

Proposition 2.1. *Suppose (a, b, c) is a primitive, non-trivial solution to the equation (2) with exponent $n \geq 17$ prime. Without loss of generality, suppose that ac is even. Then*

(i) *c is odd,*
(ii) *$\mathrm{ord}_2(a) = 1$,*
(iii) *$\mathrm{ord}_3(c) \geq 1$.*

Moreover, let $E_{a,b}$ and E be the elliptic curves given in (4) and (5). Then, for any prime $\ell \neq 2, 3$,

$$\begin{cases} a_\ell(E_{a,b}) \equiv a_\ell(E) \pmod{n} & \text{if } \ell \nmid c, \\ \ell + 1 \pm a_\ell(E) \equiv 0 \pmod{n} & \text{if } \ell \mid c. \end{cases}$$

Proof. The first part of the proposition is Théorème 6.1 of Kraus' [23]. Proposition 6.3 of the same paper asserts that $\varrho_{a,b}$ is isomorphic to the Galois representation ϱ on the n-torsion of E. It turns out that $\ell \neq 2, 3$ is a prime of good reduction if $\ell \nmid c$, and is of multiplicative reduction if $\ell \mid c$ (see Lemma 4.1 of the same paper). The second part of the proposition follows. □

We shall also need a refined version of the last part of Proposition 2.1.

Corollary 2.2. *Suppose (a, b, c) is a primitive, non-trivial solution to the equation (2) with exponent $n \geq 17$ prime. In view of Proposition 2.1 suppose, without loss of generality, that a is even. Let $\ell \neq 2, 3$ be a prime satisfying $n > (\sqrt{\ell} + 1)^2$. Then $\ell \nmid c$ and $a_\ell(E_{a,b}) = a_\ell(E)$.*

Proof. Suppose $\ell \mid c$. By the last part of Proposition 2.1, n divides $\ell + 1 \pm a_\ell(E)$. However, by the Hasse–Weil bounds,

$$0 < \ell + 1 \pm a_\ell(E) \leq (\sqrt{\ell} + 1)^2.$$

This contradicts the assumption that $n > (\sqrt{\ell} + 1)^2$. Thus $\ell \nmid c$.

Applying again the last part of Proposition 2.1, we see that n divides the difference $a_\ell(E_{a,b}) - a_\ell(E)$. Suppose $a_\ell(E_{a,b}) \neq a_\ell(E)$. Then

$$n \leq |a_\ell(E_{a,b}) - a_\ell(E)| \leq 4\sqrt{\ell} \leq (\sqrt{\ell} + 1)^2,$$

where we have again used the Hasse–Weil bounds. This contradiction completes the proof. □

We shall also need the following lemma which appears in Kraus' paper, but for convenience we give the proof.

Lemma 2.3. *Let (a, b, c) be a primitive, non-trivial solution to equation (2), and in view of Proposition 2.1, suppose that a is even. Then,*

$$a + b = \frac{c_1^n}{3}, \qquad a^2 - ab + b^2 = 3c_2^n \tag{6}$$

where c_1, c_2 are coprime integers, with $3 \mid c_1$, and $c = c_1c_2$.

Proof. In view of the earlier results on (2) cited in the introduction, n must be divisible by some prime $p > 10^4$. Proposition 2.1 holds with p in place of n and $c^{n/p}$ in place of c. In particular $3 \mid c$, and so one of $a+b$ and a^2-ab+b^2 is divisible by 3. From the identity

$$4(a^2 - ab + b^2) = 3(a - b)^2 + (a + b)^2, \tag{7}$$

we see that both $a + b$ and $a^2 - ab + b^2$ are divisible by 3, and the coprimality of a, b ensures that $9 \nmid (a^2 - ab + b^2)$. This proves the lemma. □

3. The First Hyperelliptic Curve

We shall henceforth suppose that n is odd and that (a, b, c) is a primitive, non-trivial solution to (2). In view of Proposition 2.1 we suppose, without loss of generality, that a is even.

Let c_1 and c_2 be as in Lemma 2.3 and write

$$x = 9(a - b), \qquad \epsilon = \frac{c_2}{c_1^2}, \qquad \delta = \frac{x}{9c_1^n}. \tag{8}$$

From the identity (7), we obtain

$$x^2 + 3c_1^{2n} = 324c_2^n. \tag{9}$$

Dividing by $81c_1^{2n}$ we obtain the rational point (ϵ, δ) on the hyperelliptic curve (3) mentioned in the introduction. We have included the hyperelliptic curve (3) as a motivational link between the current paper and the ideas in [8]. However, for what follows, it is more convenient to work with "projective model"(9).

Remark. Equation (9) is a ternary equation of signature $(n, n, 2)$. For this class of ternary equation, a Frey curve is given by Bennett and Skinner [4], and two Frey curves by Ivorra and Kraus [22]. However, up to isogenies and twisting, all these Frey curves are the same as Kraus' original Frey curve $E_{a,b}$, and they do not give any additional information.

We will need the following lemma.

Lemma 3.1. *Suppose the exponent n in (2) is odd. Then $\left(\frac{c_2}{3}\right) = 1$.*

Proof. By equation (9), and the facts $x = 9(a - b)$ and $3 \mid c_1$ we see that

$$4c_2^n \equiv (a - b)^2 \pmod{3^{2n-3}}.$$

□

4. Proof of a Special Case of Theorem 1

The proof of Theorem 1 requires a rather complicated combination of quadratic reciprocity over number fields with new information at several primes given by the modular approach. By 'new' we mean over and above the 2-adic and 3-adic information given in Proposition 2.1. In order to motivate this and help the reader follow the proof, we will in this section prove the following special case which involves only quadratic reciprocity over the rationals, and new information given by the modular approach at only one prime.

Special Case of Theorem 1. *If n is divisible by a positive integer $d \equiv 51$, 103 or 105 (mod 106) then equation (2) does not have non-trivial primitive solutions.*

Lemma 4.1. $\left(\dfrac{c_2 - c_1^2}{107}\right) = 0 \quad or \quad 1.$

Proof. Subtracting $324c_1^{2n}$ from both sides of equation (9) we obtain

$$x^2 - 321c_1^{2n} = 324(c_2^n - c_1^{2n}) = 324(c_2 - c_1^2)(c_2^{n-1} + \cdots).$$

Suppose q is an odd prime dividing $c_2 - c_1^2$. Since c_1, c_2 are coprime, if follows that $q \nmid c_1$. Thus 321 is a square modulo q; in symbols

$$\left(\frac{321}{q}\right) = 0 \quad \text{or} \quad 1.$$

By the Law of Quadratic Reciprocity,

$$\left(\frac{q}{321}\right) = 0 \quad \text{or} \quad 1.$$

However $\left(\dfrac{-1}{321}\right) = \left(\dfrac{2}{321}\right) = 1$. Hence $\left(\dfrac{c_2 - c_1^2}{321}\right) = 0$ or 1. Since $321 = 3 \times 107$, the lemma follows from Lemma 3.1 and the fact that $3 \mid c_1$ stated in Lemma 2.3. □

We will suppose without loss of generality that a is even, and in view of the partial results stated in the introduction that the exponent n is odd and divisible by some prime $p > 10^4$. Applying Corollary 2.2 with n replaced by p and c by $c^{n/p}$ immediately shows that

$$107 \nmid (a^3 + b^3) \qquad \text{and} \qquad a_{107}(E_{a,b}) = a_{107}(E) = 12,$$

where $E_{a,b}$ and E are given by (4) and (5).

Now let ϵ be given by (8). From (6) we have that

$$\epsilon^n = \frac{a^2 - ab + b^2}{27(a+b)^2}.$$

From the above, 107 divides neither the numerator nor the denominator of ϵ. Denote the reduction of ϵ in $\mathbb{F}_{107}$ by $\overline{\epsilon}$. Then $\overline{\epsilon}^n$ belongs to the set

$$\mathcal{E} = \left\{ \frac{\alpha^2 - \alpha\beta + \beta^2}{27(\alpha+\beta)^2} \ : \ \alpha, \beta \in \mathbb{F}_{107}, \quad \alpha^3 + \beta^3 \neq 0, \quad a_{107}(E_{\alpha,\beta}) = 12 \right\}.$$

A short `MAGMA` computation shows that

$$\mathcal{E} = \{\overline{13}, \overline{14}, \overline{36}, \overline{37}, \overline{48}, \overline{57}, \overline{62}\} \subset \mathbb{F}_{107}.$$

The following lemma clearly completes the proof of the special case of Theorem 1 that we are concerned with.

Lemma 4.2. *With notation and assumptions as above, if* $n \equiv 51, 103, 105 \pmod{106}$, *then* (2) *has no primitive, non-trivial solutions.*

Proof. For now we merely suppose that n is odd, and write $n = 106Q + R^*$ where $1 \leq R^* \leq 105$. We know by the previous results of Kraus that $53 \nmid n$, and so $\gcd(R^*, 106) = 1$. Denote by R the least positive integer such that $RR^* \equiv 1 \pmod{106}$. Thus $nR \equiv 1 \pmod{106}$, and so

$$(\overline{\epsilon}^n)^R = \overline{\epsilon} \qquad (\text{in } \mathbb{F}_{107}).$$

Recall that $\overline{\epsilon}^n \in \mathcal{E}$. Let

$$S_R = \{\overline{\alpha}^R : \overline{\alpha} \in \mathcal{E}\} \subset \mathbb{F}_{107};$$

it is clear from the above that $\overline{\epsilon} \in S_R$. Finally, let

$$S'_R = \left\{\overline{\beta} \in S_R : \left(\frac{\beta - 1}{107}\right) = 0 \quad \text{or} \quad 1\right\}.$$

By Lemma 4.1 and the fact that $\epsilon = c_2/c_1^2$, we see that $\overline{\epsilon} \in S'_R$. We wrote a short `MAGMA` script which for each $1 \leq R^* \leq 106$ with $\gcd(R^*, 106) = 1$ computed R, S_R and S'_R; the result of this computation is given in Table 1. Note that S'_R is empty for $R^* = 51, 103, 105$ (and non-empty for all other values of R^*), hence we have a contradiction for $n \equiv 51, 103, 105 \pmod{106}$. □

5. Law of Quadratic Reciprocity over Number Fields

We shall need some version of the Law of Quadratic Reciprocity over arbitrary number fields. Useful references here are the "Brighton Book" [9, pages 348–353] and Hecke's classic [21, Chapter VIII]. We first define quadratic residue symbols over number fields. Let $\mathbb{K}$ be a number field with integer ring $\mathcal{O}$. An integer or ideal of $\mathcal{O}$ is said to be *odd* if it is coprime to $2\mathcal{O}$. If $\mathfrak{P}$ is an odd prime ideal and $\alpha \in \mathcal{O}$ then we define

$$\left(\frac{\alpha}{\mathfrak{P}}\right)_{\mathbb{K}} = \begin{cases} 0 & \text{if } \mathfrak{P} \mid \alpha, \\ 1 & \text{if the image of } \alpha \text{ in } (\mathcal{O}/\mathfrak{P})^\times \text{ is a square}, \\ -1 & \text{otherwise.} \end{cases}$$

If $\mathfrak{N}$ is an odd ideal, we write $\mathfrak{N} = \mathfrak{P}_1 \cdots \mathfrak{P}_n$ as a product of odd prime ideals, and we extend the definition of the quadratic residue symbol by

$$\left(\frac{\alpha}{\mathfrak{N}}\right)_{\mathbb{K}} = \left(\frac{\alpha}{\mathfrak{P}_1}\right)_{\mathbb{K}} \cdots \left(\frac{\alpha}{\mathfrak{P}_n}\right)_{\mathbb{K}}.$$

The symbol satisfies the following familiar properties

$$\left(\frac{\alpha_1\alpha_2}{\mathfrak{N}}\right)_{\mathbb{K}} = \left(\frac{\alpha_1}{\mathfrak{N}}\right)_{\mathbb{K}} \left(\frac{\alpha_2}{\mathfrak{N}}\right)_{\mathbb{K}}, \qquad \left(\frac{\alpha}{\mathfrak{N}_1\mathfrak{N}_2}\right)_{\mathbb{K}} = \left(\frac{\alpha}{\mathfrak{N}_1}\right)_{\mathbb{K}} \left(\frac{\alpha}{\mathfrak{N}_2}\right)_{\mathbb{K}},$$

and

$$\left(\frac{\alpha_1}{\mathfrak{N}}\right)_{\mathbb{K}} = \left(\frac{\alpha_2}{\mathfrak{N}}\right)_{\mathbb{K}} \qquad \text{if } \alpha_1 \equiv \alpha_2 \pmod{\mathfrak{N}}.$$

If β is an odd integer in $\mathcal{O}$ then we define

$$\left(\frac{\alpha}{\beta}\right)_{\mathbb{K}} = \left(\frac{\alpha}{\beta\mathcal{O}}\right)_{\mathbb{K}}.$$

There are several versions of the Law of Quadratic Reciprocity over number fields. The following is the most useful to us.

TABLE 1. The table gives the computational results for Lemma 4.2.

R^*	R	S_R	S'_R
1	1	$\{36, 37, 57, 62, 13, 14, 48\}$	$\{36, 37, 57, 62, 13, 14, 48\}$
3	71	$\{13, 40, 30, 41, 86, 10, 76\}$	$\{13, 40, 30, 41, 86, 10, 76\}$
5	85	$\{33, 44, 12, 34, 36, 40, 10\}$	$\{12, 34, 36, 40, 10\}$
7	91	$\{99, 100, 90, 47, 4, 16, 64\}$	$\{100, 90, 4\}$
9	59	$\{23, 16, 39, 83, 52, 41, 53\}$	$\{41, 53\}$
11	29	$\{89, 35, 57, 3, 69, 16, 53\}$	$\{35, 57, 53\}$
13	49	$\{11, 14, 102, 36, 81, 40, 86\}$	$\{11, 14, 102, 36, 40, 86\}$
15	99	$\{44, 47, 61, 52, 30, 53, 42\}$	$\{30, 53, 42\}$
17	25	$\{100, 92, 29, 41, 53, 87, 10\}$	$\{100, 41, 53, 87, 10\}$
19	67	$\{35, 90, 4, 48, 49, 75, 76\}$	$\{35, 90, 4, 48, 49, 76\}$
21	101	$\{11, 12, 79, 36, 4, 105, 29\}$	$\{11, 12, 36, 4\}$
23	83	$\{102, 87, 25, 76, 10, 79, 83\}$	$\{102, 87, 76, 10\}$
25	17	$\{33, 90, 69, 61, 19, 53, 64\}$	$\{90, 53\}$
27	55	$\{99, 12, 89, 57, 39, 62, 85\}$	$\{12, 57, 62\}$
29	11	$\{100, 12, 102, 37, 19, 86, 10\}$	$\{100, 12, 102, 37, 86, 10\}$
31	65	$\{23, 101, 27, 29, 41, 42, 76\}$	$\{101, 41, 42, 76\}$
33	45	$\{34, 102, 89, 25, 12, 13, 14\}$	$\{34, 12, 13, 102, 14\}$
35	103	$\{11, 100, 79, 92, 27, 49, 76\}$	$\{11, 100, 49, 76\}$
37	43	$\{12, 35, 14, 92, 37, 4, 16\}$	$\{12, 35, 14, 37, 4\}$
39	87	$\{27, 83, 40, 30, 19, 75, 53\}$	$\{40, 30, 53\}$
41	75	$\{100, 13, 25, 37, 49, 40, 85\}$	$\{100, 13, 37, 49, 40\}$
43	37	$\{89, 90, 3, 25, 37, 62, 86\}$	$\{90, 37, 62, 86\}$
45	33	$\{11, 89, 37, 48, 16, 85, 42\}$	$\{11, 37, 48, 42\}$
47	97	$\{56, 90, 102, 47, 49, 62, 85\}$	$\{90, 102, 49, 62\}$
49	13	$\{56, 57, 14, 3, 52, 85, 42\}$	$\{57, 14, 42\}$
51	79	$\{33, 89, 56, 39, 29, 52, 9\}$	$\emptyset$
55	27	$\{11, 12, 101, 13, 35, 48, 86\}$	$\{11, 12, 101, 13, 35, 48, 86\}$
57	93	$\{23, 34, 35, 79, 36, 92, 86\}$	$\{34, 35, 36, 86\}$
59	9	$\{44, 34, 83, 41, 19, 64, 86\}$	$\{34, 41, 86\}$
61	73	$\{34, 101, 79, 81, 39, 29, 87\}$	$\{34, 101, 87\}$
63	69	$\{44, 56, 101, 36, 81, 19, 30\}$	$\{101, 36, 30\}$
65	31	$\{99, 33, 34, 81, 83, 61, 30\}$	$\{34, 30\}$
67	19	$\{99, 25, 4, 49, 105, 62, 10\}$	$\{4, 49, 62, 10\}$
69	63	$\{23, 57, 81, 27, 52, 9, 87\}$	$\{57, 87\}$
71	3	$\{57, 69, 4, 83, 39, 61, 42\}$	$\{57, 4, 42\}$
73	61	$\{33, 23, 101, 85, 30, 64, 9\}$	$\{101, 30\}$
75	41	$\{69, 89, 4, 79, 47, 14, 48\}$	$\{14, 4, 48\}$
77	95	$\{56, 81, 61, 62, 64, 75, 9\}$	$\{62\}$
79	51	$\{11, 34, 101, 92, 40, 19, 9\}$	$\{11, 34, 101, 40\}$
81	89	$\{44, 100, 13, 102, 105, 62, 76\}$	$\{100, 13, 102, 62, 76\}$
83	23	$\{69, 75, 42, 30, 64, 49, 16\}$	$\{49, 30, 42\}$
85	5	$\{3, 48, 27, 39, 9, 42, 53\}$	$\{48, 42, 53\}$
87	39	$\{44, 69, 27, 83, 29, 52, 10\}$	$\{10\}$
89	81	$\{57, 47, 48, 16, 105, 61, 75\}$	$\{57, 48\}$
91	7	$\{100, 90, 35, 79, 25, 105, 41\}$	$\{100, 90, 35, 41\}$
93	57	$\{99, 56, 23, 3, 37, 39, 64\}$	$\{37\}$
95	77	$\{101, 36, 92, 105, 52, 87, 76\}$	$\{101, 36, 87, 76\}$
97	47	$\{11, 35, 47, 14, 49, 105, 87\}$	$\{11, 35, 14, 49, 87\}$
99	15	$\{44, 102, 27, 61, 40, 41, 87\}$	$\{102, 40, 41, 87\}$
101	21	$\{99, 13, 90, 3, 85, 9, 75\}$	$\{13, 90\}$
103	35	$\{69, 56, 75, 25, 47, 99, 33\}$	$\emptyset$
105	105	$\{33, 23, 3, 81, 92, 29, 19\}$	$\emptyset$

Theorem 3. *With the above notation, suppose $\mathbb{K}$ has r real embeddings. For $\alpha \in \mathbb{K}$ we write $\operatorname{sgn}_i(\alpha)$ for the sign of the image of α under the i-th real embedding. Let α, λ be coprime integers with α odd. Decompose $\lambda\mathcal{O} = \mathfrak{L}\mathfrak{R}$ where $\mathfrak{R}$ is an odd ideal. Suppose α is a quadratic residue modulo $4\mathfrak{L}$. Then*

$$\left(\frac{\lambda}{\alpha}\right)_{\mathbb{K}} \left(\frac{\alpha}{\mathfrak{R}}\right)_{\mathbb{K}} = (-1)^{\sigma}$$

where

$$\sigma = \sum_{i=1}^{r} \frac{\operatorname{sgn}_i(\alpha) - 1}{2} \cdot \frac{\operatorname{sgn}_i(\lambda) - 1}{2}.$$

Proof. This is Theorem 167 of [21]. □

Corollary 5.1. *Let α, λ be integers in number field $\mathbb{K}$ with α odd. Suppose that $\alpha \equiv \epsilon^2 \pmod{4\lambda}$ for some integer ϵ. Suppose also that α is positive in every real embedding of $\mathbb{K}$ (this would be vacuously true if $\mathbb{K}$ is totally complex). Then*

$$\left(\frac{\lambda}{\alpha}\right)_{\mathbb{K}} \neq -1.$$

Proof. If α and λ are not coprime, then $\left(\frac{\lambda}{\alpha}\right)_{\mathbb{K}} = 0$. Otherwise we apply Theorem 3 with $\mathfrak{L} = \lambda\mathcal{O}$ and $\mathfrak{R} = (1)$. □

If $\epsilon = \alpha/\beta$ where α, β are integers, with β, $\mathfrak{N}$ coprime, then we extend the definition of the quadratic residue symbol by letting

$$\left(\frac{\epsilon}{\mathfrak{N}}\right)_{\mathbb{K}} = \left(\frac{\alpha}{\mathfrak{N}}\right)_{\mathbb{K}} \left(\frac{\beta}{\mathfrak{N}}\right)_{\mathbb{K}}.$$

We shall later on deal with quadratic reciprocity in several fields, and it is appropriate to emphasize the field dependence of the quadratic residue symbol. Although we shall not need it, it is useful to note that if α, $\beta \in \mathbb{K}$ and $\mathbb{L}$ contains $\mathbb{K}$ then

$$\left(\frac{\alpha}{\beta}\right)_{\mathbb{L}} = \left(\frac{\alpha}{\beta}\right)_{\mathbb{K}}^{[\mathbb{L}:\mathbb{K}]}.$$

6. Two More Hyperelliptic Curves

We shall continue with the notation of Section 3. Let $\omega = (-1 + \sqrt{-3})/2$; that is, ω is a primitive cube root of unity. Let $\mathbb{K} = \mathbb{Q}(\omega)$ and $\mathcal{O}_{\mathbb{K}}$ be its ring of integers. We can extend the earlier factorization (6) to

$$a + b = \frac{c_1^n}{3}, \qquad a + \omega b = \sqrt{-3}\gamma^n, \qquad a + \overline{\omega} b = -\sqrt{-3}\overline{\gamma}^n \tag{10}$$

where $\gamma \in \mathcal{O}_{\mathbb{K}}$ and $\gamma\overline{\gamma} = c_2$. We employ the identity

$$3(a - \overline{\omega}b)^2 + (a + \overline{\omega}b)^2 = 4(a + b)(a + \omega b).$$

We ease notation a little by letting

$$A = 3(a - \overline{\omega}b), \qquad B = c_1\gamma.$$

Using the identity we obtain our second hyperelliptic equation,

$$A^2 - 9\overline{\gamma}^{2n} = 4\sqrt{-3}B^n. \tag{11}$$

Conjugating we obtain our third,

$$\overline{A}^2 - 9\gamma^{2n} = -4\sqrt{-3}\,\overline{B}^n. \tag{12}$$

Now let

$$\mu = \frac{B}{\overline{\gamma}^2}, \qquad \nu = \frac{A}{\overline{\gamma}^n}. \tag{13}$$

The our second and third hyperelliptic equations can be written in the form

$$\nu^2 - 9 = 4\sqrt{-3}\mu^n, \qquad \overline{\nu}^2 - 9 = -4\sqrt{-3}\overline{\mu}^n.$$

Remark. There are "associated" $\mathbb{Q}$-curves to the equations (11) and (12) but they turn out to be isogenous over $\overline{\mathbb{Q}}$ to the standard Frey elliptic curve over $\mathbb{Q}$ used in Kraus so no new modular information is obtained (cf. also the remark in Section 3). This is consistent with the classification of Frey representations for the equation $x^3 + y^3 = z^p$ in [16].

7. Reciprocity

We continue with the notation of the previous section. In particular $\mathbb{K} = \mathbb{Q}(\omega)$, where ω is a primitive cube root of unity. Now let r be a positive integer coprime to n, and let ζ_r be a primitive r-th root of unity. Let

$$\mathbb{L} = \mathbb{Q}(\zeta_r), \qquad \mathbb{M} = \mathbb{K}(\zeta_r) = \mathbb{Q}(\omega, \zeta_r).$$

Let n' be a positive integer satisfying $nn' \equiv 1 \pmod{r}$, and let $\zeta_r' = \zeta_r^{n'}$. Thus $\zeta_r = \zeta_r'^{\,n}$.

Proposition 7.1. *With notation as above, let p be the largest prime dividing n, where n is the exponent appearing in equation* (2).

(I) *Suppose that $p > (\sqrt{\ell}+1)^2$ for all primes $\ell \mid \mathrm{Norm}_{\mathbb{L}/\mathbb{Q}}(108\zeta_r - 1)$. Let ϵ be given by* (8). *Then $108\zeta_r - 1$ is coprime with the denominator of ϵ and*

$$\left(\frac{\epsilon - \zeta_r'}{108\zeta_r - 1}\right)_{\mathbb{L}} \neq -1.$$

(II) *Suppose that $p > (\sqrt{\ell}+1)^2$ for all primes $\ell \mid \mathrm{Norm}_{\mathbb{M}/\mathbb{Q}}(4\zeta_r - 3\sqrt{-3})$. Let μ be given by* (13). *Then $4\zeta_r - 3\sqrt{-3}$ is coprime with the denominator of μ and*

$$\left(\frac{\mu - \zeta_r'}{4\zeta_r - 3\sqrt{-3}}\right)_{\mathbb{M}} \left(\frac{-\zeta_r'}{\sqrt{-3}}\right)_{\mathbb{M}} \neq -1, \quad \textit{and} \quad \left(\frac{\overline{\mu} + \zeta_r'}{4\zeta_r - 3\sqrt{-3}}\right)_{\mathbb{M}} \left(\frac{\zeta_r'}{\sqrt{-3}}\right)_{\mathbb{M}} \neq -1.$$

Proof. We first prove the coprimality statements. The denominator of ϵ is c_1^2. Suppose that is not coprime with $108\zeta_r - 1$. Then there is some rational prime ℓ dividing both $\mathrm{Norm}_{\mathbb{L}/\mathbb{Q}}(108\zeta_r - 1)$ and $c = c_1c_2$. Clearly $\ell \neq 2$, 3. Now applying Corollary 2.2 with p instead of n gives an immediate contradiction. This proves the coprimality statement in (I). For (II) the proof of the coprimality statement is identical since $c = c_1\gamma\overline{\gamma}$ and the denominator of μ is $\overline{\gamma}^2$. The proposition now follows at once from Lemmas 7.2 and 7.3 below and the definitions of ϵ and μ in (8) and (13). □

Lemma 7.2.

$$\left(\frac{c_2 - c_1^2\zeta_r'}{108\zeta_r - 1}\right)_{\mathbb{L}} \neq -1.$$

Proof. Subtracting $324c_1^{2n}\zeta_r$ from both sides of equation (9) we obtain

$$x^2 + (3 - 324\zeta_r)c_1^{2n} = 4 \times 81(c_2^n - c_1^{2n}\zeta_r).$$

Recall however that $\zeta_r = {\zeta'_r}^n$. Hence

$$x^2 - (324\zeta_r - 3)c_1^{2n} = 4(c_2 - c_1^2\zeta'_r) \times 81(c_2^{n-1} + \cdots).$$

Now, by Lemma 2.3, c_1, c_2 are coprime, $3 \mid c_1$ and $3 \nmid c_2$. Thus $c_2 - c_1^2\zeta'_r$ and c_1^{2n} are coprime. Moreover, by Proposition 2.1, $c = c_1c_2$ is odd. It follows that $324\zeta_r - 3$ is a square modulo $4(c_2 - c_1^2\zeta'_r)$. Applying Corollary 5.1 we see that

$$\left(\frac{c_2 - c_1^2\zeta'_r}{324\zeta_r - 3}\right)_{\mathbb{L}} \neq -1.$$

However, from the proof of Lemma 3.1 we find that c_2 is a quadratic residue modulo every prime ideal dividing $3\mathcal{O}_{\mathbb{L}}$ (recall our assumption that n is odd). Hence

$$\left(\frac{c_2 - c_1^2\zeta'_r}{3}\right)_{\mathbb{L}} = 1.$$

The lemma follows since $324\zeta_r - 3 = 3(108\zeta_r - 1)$. □

Lemma 7.3.

$$\left(\frac{B - \zeta'_r\overline{\gamma}^2}{4\zeta_r - 3\sqrt{-3}}\right)_{\mathbb{M}} \left(\frac{-\zeta'_r}{\sqrt{-3}}\right)_{\mathbb{M}} \neq -1,$$

and

$$\left(\frac{\overline{B} + \zeta'_r\gamma^2}{4\zeta_r - 3\sqrt{-3}}\right)_{\mathbb{M}} \left(\frac{\zeta'_r}{\sqrt{-3}}\right)_{\mathbb{M}} \neq -1.$$

Proof. The proof if very similar to that of Lemma 7.2. Subtracting $4\sqrt{-3}\overline{\gamma}^{2n}\zeta_r = 4\sqrt{-3}\overline{\gamma}^{2n}{\zeta'_r}^n$ from both sides of (11) we obtain

$$A^2 - (9 + 4\sqrt{-3}\zeta_r)\overline{\gamma}^{2n} = 4\sqrt{-3}(B - \zeta'_r\overline{\gamma}^2)(B^{n-1} + \cdots).$$

Also subtracting $4\sqrt{-3}\gamma^{2n}\zeta_r$ from both sides we of (12) gives

$$\overline{A}^2 - (9 + 4\sqrt{-3}\zeta_r)\gamma^{2n} = -4\sqrt{-3}(\overline{B} + \zeta'_r\gamma^2)(\overline{B}^{n-1} + \cdots).$$

We shall only prove the first part of the lemma; the proof of the second part is almost identical. Corollary 5.1 gives

$$\left(\frac{B - \zeta'_r\overline{\gamma}^2}{9 + 4\sqrt{-3}\zeta_r}\right)_{\mathbb{M}} \neq -1.$$

Note that

$$\left(\frac{B - \zeta'_r\overline{\gamma}^2}{9 + 4\sqrt{-3}\zeta_r}\right)_{\mathbb{M}} = \left(\frac{B - \zeta'_r\overline{\gamma}^2}{4\zeta_r - 3\sqrt{-3}}\right)_{\mathbb{M}} \left(\frac{B - \zeta'_r\overline{\gamma}^2}{\sqrt{-3}}\right)_{\mathbb{M}}.$$

However, $\sqrt{-3} \mid B$. Further γ and $\sqrt{-3}$ are coprime as $3 \nmid c_2 = \gamma\overline{\gamma}$. Hence

$$\left(\frac{B - \zeta'_r\overline{\gamma}^2}{\sqrt{-3}}\right)_{\mathbb{M}} = \left(\frac{-\zeta'_r}{\sqrt{-3}}\right)_{\mathbb{M}}.$$

This completes the proof. □

8. Combination of Reciprocity and Modularity

In this section we state our main result, Proposition 8.1, which combines reciprocity with the information given by the modular approach.

We shall need a way of storing information given by the modular approach employing several auxiliary primes ℓ. Let $\ell \neq 2, 3$ be a prime. Fix a quadratic non-residue q_ℓ modulo ℓ and let

$$\mathcal{A}'_\ell = \{(0,1),(0,q_\ell)\} \cup \{(\alpha,\beta) : \alpha = 1, q_\ell, \quad \beta = 0, 1, \ldots, (\ell-1)\}.$$

Let

$$\mathcal{A}_\ell = \{(\alpha,\beta) \in \mathcal{A}'_\ell : \alpha^3 + \beta^3 \not\equiv 0 \pmod{\ell} \quad \text{and} \quad a_\ell(E_{\alpha,\beta}) = a_\ell(E)\}.$$

Now let $S = \{\ell_1, \ldots, \ell_t\}$ be a set of distinct primes, all $\neq 2, 3$, and write $L_S = \prod_{i=1}^t \ell_i$. Let $\mathcal{A}_S$ be the set of (α,β) with $0 \leq \alpha, \beta < L_S$, such that, for all i, (α,β) reduces to an element of $\mathcal{A}_{\ell_i}$ modulo ℓ_i.

For $\alpha, \beta \in \mathcal{A}_S$, let

$$f(\alpha,\beta) = \frac{\alpha^2 - \alpha\beta + \beta^2}{27(\alpha+\beta)^2}, \qquad g(\alpha,\beta) = \frac{3\sqrt{-3}(\alpha+\beta)(\alpha+\beta\omega)}{(\alpha+\beta\overline{\omega})^2}. \tag{14}$$

For $(\alpha,\beta) \in \mathcal{A}_S$, r-th root of unity ζ_r, and integer R we define

$$\theta_{\zeta_r}(\alpha,\beta,R) = \left(\frac{f(\alpha,\beta)^R - \zeta_r^R}{108\zeta_r - 1}\right)_{\mathbb{L}}, \tag{15}$$

$$\phi_{\zeta_r}(\alpha,\beta,R) = \left(\frac{g(\alpha,\beta)^R - \zeta_r^R}{4\zeta_r - 3\sqrt{-3}}\right)_{\mathbb{M}} \left(\frac{-\zeta_r^R}{\sqrt{-3}}\right)_{\mathbb{M}}, \tag{16}$$

$$\psi_{\zeta_r}(\alpha,\beta,R) = \left(\frac{\overline{g(\alpha,\beta)}^R + \zeta_r^R}{4\zeta_r - 3\sqrt{-3}}\right)_{\mathbb{M}} \left(\frac{\zeta_r^R}{\sqrt{-3}}\right)_{\mathbb{M}}. \tag{17}$$

We associate to θ_{ζ_r}, ϕ_{ζ_r}, ψ_{ζ_r} the following positive integers

$$N(\theta_{\zeta_r}) = \operatorname{lcm}\left(\#(\mathcal{O}_{\mathbb{L}}/(108\zeta_r - 1))^\times, r\right),$$
$$N(\phi_{\zeta_r}) = N(\psi_{\zeta_r}) = \operatorname{lcm}\left(\#(\mathcal{O}_{\mathbb{M}}/(4\zeta_r - 3\sqrt{-3}))^\times, r\right).$$

We say that θ_{ζ_r} is a *S-admissible* if $(108\zeta_r - 1) \mid L_S$. We say that ϕ_{ζ_r}, ψ_{ζ_r} are *S-admissible* if $(4\zeta_r - 3\sqrt{-3}) \mid L_S$.

Proposition 8.1. *Let $S = \{\ell_1, \ldots, \ell_t\}$ be a set of distinct primes, all $\neq 2, 3$. Let $\Xi = \{\xi_1, \ldots, \xi_s\}$ be a set of S-admissible functions of the form* (15), (16), (17)*, and let*

$$N = \operatorname{lcm}_{i=1}^s N(\xi_i).$$

Let $0 \leq R$, $R^* < N$ be a positive integer coprime to N, such that $RR^* \equiv 1 \pmod{N}$. Define

$$\mathcal{A}_{S,R} = \{(\alpha,\beta) \in \mathcal{A}_S : \xi_i(\alpha,\beta,R) \neq -1 \text{ for } i = 1, \ldots, s\}.$$

Suppose (a,b,c) is a non-trivial primitive solution to equation (2) *with exponent n having some prime divisor p satisfying $p > (\sqrt{\ell}+1)^2$ for all $\ell \in S$. If $n \equiv R^* \pmod{N}$ then $\mathcal{A}_{S,R} \neq \emptyset$.*

The proposition will allow us to exclude certain residue classes for the value of the exponent n in (2) modulo certain integers N. This is how we prove Theorem 1 below. Before we prove the proposition we need some lemmas.

Lemma 8.2. *Let $S = \{\ell_1, \dots, \ell_t\}$ be a set of distinct primes, all $\neq 2$, 3. Suppose (a, b, c) is a non-trivial primitive solution to equation (2). In view of Proposition 2.1 suppose, without loss of generality, that a is even. Suppose that the exponent n is divisible by some prime p satisfying $p > (\sqrt{\ell_i} + 1)^2$, for all i. Then there is some integer λ not divisible by any ℓ_i, and $(\alpha, \beta) \in \mathcal{A}_S$ such that*

$$a \equiv \lambda^2 \alpha, \qquad b \equiv \lambda^2 \beta \pmod{L_S}.$$

Proof. By the Chinese Remainder Theorem, it is clearly sufficient to prove the following statement: if $\ell \neq 2$, 3 is a prime such that $p > (\sqrt{\ell} + 1)^2$ then there is some integer λ not divisible by ℓ, and $(\alpha, \beta) \in \mathcal{A}_\ell$ such that

$$a \equiv \lambda^2 \alpha, \qquad b \equiv \lambda^2 \beta \pmod{\ell}.$$

Let us prove this. Clearly there is some $\lambda \not\equiv 0 \pmod{\ell}$, and $(\alpha, \beta) \in \mathcal{A}'_\ell$ such that $a \equiv \lambda^2 \alpha$ and $b \equiv \lambda^2 \beta \pmod{\ell}$. By Corollary 2.2, $\ell \nmid c^p = a^3 + b^3$ and $a_\ell(E_{a,b}) = a_\ell(E)$. Note that the elliptic curves $E_{\alpha,\beta}$ and $E_{a,b}$ are isomorphic modulo ℓ. Thus $a_\ell(E_{a,b}) = a_\ell(E_{\alpha,\beta})$, which shows that $(\alpha, \beta) \in \mathcal{A}_\ell$. This completes the proof. □

Lemma 8.3. *Let $S = \{\ell_1, \dots, \ell_t\}$ be a set of distinct primes, all $\neq 2$, 3. Write $L_S = \prod_{i=1}^{n} \ell_i$. Suppose (a, b, c) is a non-trivial primitive solution to equation (2). Without loss of generality, suppose that ac is even. Let ϵ and μ be given by (8) and (13). Suppose that the exponent n is divisible by some prime p satisfying $p > (\sqrt{\ell_i} + 1)^2$, for all i. Then there is some $(\alpha, \beta) \in \mathcal{A}_S$ such that*

$$\epsilon^n \equiv f(\alpha, \beta) \pmod{L_S}, \qquad \mu^n \equiv g(\alpha, \beta) \pmod{L_S \mathcal{O}_K}. \tag{18}$$

Proof. A little manipulation using (8) and (6) shows that $\epsilon^n = f(a, b)$. Likewise, using (13) and (10), we have that $\mu^n = g(a, b)$. The lemma now follows from Lemma 8.2. □

8.1. **Proof of Proposition 8.1.** Suppose that $n \equiv R^* \pmod{N}$. Thus $nR \equiv 1 \pmod{N}$. We would like to show that $\mathcal{A}_{S,R} \neq \emptyset$. We work with the notation of Lemma 8.3. From that lemma we know that there is some pair $(\alpha, \beta) \in \mathcal{A}_S$ satisfying (18). It is sufficient to show that $\xi_i(\alpha, \beta, R) \neq -1$ for $i = 1, \dots, s$. Suppose first that $\xi_i = \theta_{\zeta_r}$ for some r. Since θ_{ζ_r} is S-admissible, $(108\zeta_r - 1) \mid L_S$. Thus by (18),

$$f(\alpha, \beta)^R \equiv \epsilon^{nR} \pmod{(108\zeta_r - 1)}.$$

However, $nR \equiv 1 \pmod{N}$ and N is divisible by the order of the multiplicative group $(\mathcal{O}_{\mathbb{L}}/(108\zeta_r - 1))^\times$. Thus

$$f(\alpha, \beta)^R \equiv \epsilon \pmod{(108\zeta_r - 1)}.$$

Also, N is divisible by r, so $nR \equiv 1 \pmod{r}$ which shows that $R \equiv n' \pmod{r}$ in the notation of Section 7. Hence $\zeta_r^R = \zeta_r^{n'} = \zeta'_r$. Thus

$$\theta_{\zeta_r}(\alpha, \beta, R) = \left(\frac{\epsilon - \zeta'_r}{108\zeta_r - 1} \right)_{\mathbb{L}}.$$

Appealing to the first part of Proposition 7.1 shows that $\theta_{\zeta_r}(\alpha, \beta, R) \neq -1$, completing the proof for $\xi_i = \theta_{\zeta_r}$.

Suppose now that ξ_i is one of ϕ_{ζ_r}, ψ_{ζ_r}. By (18)

$$g(\alpha, \beta)^R \equiv \mu^{nR} \pmod{L_S \mathcal{O}_{\mathbb{M}}}.$$

As L_S is a rational integer, we see that

$$\overline{g(\alpha,\beta)}^R \equiv \overline{\mu}^{nR} \pmod{L_S\mathcal{O}_{\mathbb{M}}},$$

as well. Now ξ_i is S-admissible, so $(4\zeta_r - 3\sqrt{-3}) \mid L_S$. Moreover, $nR \equiv 1 \pmod{N}$ and N is divisible by the order of the multiplicative group $(\mathcal{O}_{\mathbb{M}}/(4\zeta_r - 3\sqrt{-3}))^\times$. Thus

$$g(\alpha,\beta)^R \equiv \mu, \qquad \overline{g(\alpha,\beta)}^R \equiv \overline{\mu} \pmod{(4\zeta_r - 3\sqrt{-3})}.$$

As above, $\zeta_r^R = \zeta_r'$. From (16) and (17),

$$\phi_{\zeta_r}(\alpha,\beta,R) = \left(\frac{\mu - \zeta_r'}{4\zeta_r - 3\sqrt{-3}}\right)_{\mathbb{M}} \left(\frac{-\zeta_r'}{\sqrt{-3}}\right)_{\mathbb{M}},$$
$$\psi_{\zeta_r}(\alpha,\beta,R) = \left(\frac{\overline{\mu} + \zeta_r'}{4\zeta_r - 3\sqrt{-3}}\right)_{\mathbb{M}} \left(\frac{\zeta_r'}{\sqrt{-3}}\right)_{\mathbb{M}}.$$

Finally, appealing to the second part of Proposition 7.1, shows that $\xi_i(\alpha,\beta,R) \neq -1$ as desired. This completes the proof.

9. Proof of Theorem 1

The theorem is proved by applying Proposition 8.1 and using the fact that we can assume without loss of generality that $n \equiv R^* \pmod{N}$ for $\gcd(R^*, N) = 1$ in the cases considered. First we shall take $S = \{11\}$. We may assume that n is odd and by previous results of Kraus and others we know that n must be divisible by some prime $p > 10^4$, and this is certainly greater than $(\sqrt{11}+1)^2$.

We shall work with $\Xi = \{\phi_{\sqrt{-1}}, \psi_{\sqrt{-1}}\}$. Note that $11 = -(4\sqrt{-1} - 3\sqrt{-3})(4\sqrt{-1} + 3\sqrt{-3})$, hence the two functions in Ξ are S-admissible. Using a short `MAGMA` script we determined

$$\mathcal{A}_S = \mathcal{A}_{11} = \{(2,1),(2,4)\}.$$

It is easy to see that $N = 120$. For the 32 values of R^* satisfying $0 \leq R^* < 120$ and $\gcd(R^*, 120) = 1$ we computed R and $\mathcal{A}_{S,R}$. We found that $\mathcal{A}_{S,R}$ is empty precisely when

$$R^* \equiv 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 77, 83, 97, 103, 107, 113 \pmod{120}.$$

Appealing to Proposition 8.1, we deduce that there can be no non-trivial primitive solutions to (2) when n is congruent to one of these values of R^* modulo 120. Note that these are precisely the values of R^* modulo 120 that reduce to 2, 3 modulo 5. This shows that there are no non-trivial primitive solutions when $n \equiv 2, 3 \pmod{5}$, and so proves part (I) of Theorem 1.

The proof of the remaining parts is similar. We quickly indicate our choices of S, Ξ. For part (II) we took $S = \{79\}$, $\zeta_6 = -\omega$ a sixth-root of unity, and $\Xi = \{\phi_{\zeta_6}, \psi_{\zeta_6}\}$.

Part (III) was dealt with in Section 4, but in our new notation we point out the choices $S = \{107\}$, $\zeta_1 = 1$, and $\Xi = \{\theta_1\}$.

Finally, for part (IV) we took $S = \{13, 109\}$, and

$$\Xi = \{\theta_{-1}, \phi_{\sqrt{-1}\omega}, \psi_{\sqrt{-1}\omega}, \phi_{\sqrt{-1}\omega^2}, \psi_{\sqrt{-1}\omega^2}\}.$$

9.1. **A Remark on the Proof of Theorem 1.** The reader is probably wondering if other sets of primes S will give further results. Our experiments suggest otherwise for the reasons we now explain.

The primes belonging to S must include the primes ℓ dividing $\mathrm{Norm}(108\zeta_r - 1)$ or $\mathrm{Norm}(4\zeta_r - 3\sqrt{-3})$ depending on whether we would like to admit θ_{ζ_r} or ϕ_{ζ_r} and ψ_{ζ_r}. As r grows, these norms grow very rapidly. We see no reason why these norms should only be divisible by primes ℓ such that $\mathcal{A}_\ell$ is small. As a result, the $\mathcal{A}_S$ are typically large once we admit functions θ_{ζ_r} or ϕ_{ζ_r} and ψ_{ζ_r} with large r. Each 'distinct' admissible function can be expected to 'cut out' roughly one half of any $\mathcal{A}_{S,R}$. If $\mathcal{A}_S$ is small then with a few choices of admissible functions we can hope that for some R we have $\mathcal{A}_{S,R} = \emptyset$. However if $\mathcal{A}_S$ is large then one needs more admissible functions and this leads to an enlargement of S and so on.

We used the following strategy to find good candidates for sets of admissible functions. We performed the search on r as a product of primes ≤ 61 so that $\phi(r) \leq 60$ for θ_ζ and $\phi(3r) \leq 60$ for ϕ_ζ and ψ_ζ. As the norms $\mathrm{Norm}(108\zeta_r - 1)$ and $\mathrm{Norm}(4\zeta_r - 3\sqrt{-3})$ were difficult to factor, we used the following method.

We made a list T of all primes ℓ less than $15,000$ such that $\#\mathcal{A}_\ell \leq 50$. In order to speed up the creation of T, it was faster to simply give an upper bound on $\#\mathcal{A}_\ell$ by picking a random point on $E_{\alpha,\beta}(\mathbb{F}_\ell)$ and checking that it is annihilated by $\ell + 1 - a_\ell(E)$. If that was the case for 10 tries, we added the pair (α, β) to $\mathcal{A}_\ell$.

Next, we only factored $\mathrm{Norm}(108\zeta_r - 1)$ and $\mathrm{Norm}(4\zeta_r - 3\sqrt{-3})$ using the primes in T. If the norms were divisible by some prime ℓ not in T, it was omitted on the basis that the resulting $\#\mathcal{A}_\ell$ would probably be larger than 50.

The following table summarizes the list of candidates found. In the table, $\zeta = \zeta_r^k$ where $\zeta_r = e^{2\pi i/r}$. No new sets of admissible functions which yield results were found.

k/r	S for θ_ζ	S for ϕ_ζ, ψ_ζ
1	$\{107\}$	$\{43\}$
1/2	$\{109\}$	$\{43\}$
$\{1,3\}/4$	$\{5, 2333\}$	$\{11\}$
$\{1,3,5,7\}/8$		$\{5, 197\}$
1/3	$\{61, 193\}$	$\{7\}$
2/3	$\{61, 193\}$	$\{79\}$
1/6	$\{7, 13, 127\}$	$\{7\}$
5/6	$\{7, 13, 127\}$	$\{79\}$
$\{1,5,7,11\}/12$		$\{13, 109\}$

10. Density Results

In this section we prove the density assertions made in the introduction regarding exponents n for which satisfy the conditions of Theorem 1. Suppose first that n is prime. Then we need to evaluate the Dirichlet density of primes satisfying any of the congruences in Theorem 1. The least common multiple of the moduli 5, 78, 106 and 1296 appearing in the theorem is 4464720. Let S be the set of d in $0 \leq d < 4464720$ satisfying $\gcd(d, 4464720) = 1$ and at least one of the congruence conditions of the theorem. We computed S using a short `MAGMA` script and found that $\#S = 677256$. Thus the Dirichlet density of *prime* exponents n satisfying the

conditions of Theorem 1 is

$$\frac{\#S}{\phi(4464720)} = \frac{28219}{44928}.$$

This proves the assertion made in the introduction about the density for prime exponents n.

We would now like to prove that the set of positive integers n satisfying the conditions of Theorem 1 has natural density 1. For this it is sufficient to show that the set of positive integers n divisible by some prime $p \equiv 2 \pmod 5$ has natural density 1. Let A be a set of positive integers. For x positive, define

$$A(x) = \#\{m \in A : m \leq x\}.$$

The natural density of A is defined as the limit (if it exists)

$$\delta(A) = \lim_{x \to \infty} \frac{A(x)}{x}.$$

For a given prime p, define

$$A_p = \{m \in A : p \mid m \text{ and } p^2 \nmid m\}.$$

We shall need the following result of Niven [25, Corollary 1].

Theorem (I. Niven). *Let $\{p_i\}$ be a set of primes such that $\delta(A_{p_i}) = 0$ and $\sum p_i^{-1} = \infty$. Then $\delta(A) = 0$.*

Now we shall let A be the set of positive integers n *not divisible* by any prime $p \equiv 2 \pmod 5$. It is enough for us to prove that $\delta(A) = 0$. To show this, let $\{p_i\}$ be the set of primes $p \equiv 2 \pmod 5$. It follows from the usual proof of Dirichlet's Theorem that $\sum p_i^{-1} = \infty$. Moreover, all A_{p_i} are empty and so have density 0. Thus by Niven's result above, $\delta(A) = 0$.

11. A Refinement of Kraus' Criterion

As mentioned in the introduction, Kraus [23] gives a criterion which likely to allow one to prove that equation (2) does not have non-trivial primitive solution, for a given prime exponent n. By checking his criterion on a computer, Kraus was able prove that the equation (2) has no non-trivial primitive solution for prime exponents $17 \leq n < 10^4$. In this section we explain a refinement of Kraus' criterion which is much faster in practice. The refinement is inspired by [11, Proposition 8.2].

It is perhaps helpful if we explain the idea behind Kraus' criterion briefly. For a given prime exponent n we choose a small integer k such that $\ell = kn + 1$ is prime. Now c_1^n and c_2^n are either 0 or k-th roots of unity modulo ℓ. In either case they belong to a small set modulo ℓ. By equation (6), a, b also belong to a small set modulo ℓ. For these pairs of a, b, it is unlikely that the congruences given in Proposition 2.1 are satisfied. This idea forms the basis of Kraus' criterion.

First we seek a convenient model of the Frey curve $E_{a,b}$. Replacing X by $X+a-b$ in the model given in (4) we obtain

$$Y^2 = X^3 + 3(a-b)X^2 + 3(a^2 - ab + b^2)X.$$

Recalling our earlier notation, this is the same as the model

$$Y^2 = X^3 + \frac{x}{3}X^2 + 9c_2^n X.$$

Twisting by $3c_1^n$ we obtain the model

$$E_{\epsilon,\delta} : Y^2 = X^3 + \delta X^2 + \epsilon^n X, \tag{19}$$

where ϵ and δ are given by (8). Let k be an integer such that $\ell = kn + 1$ is prime. Define

$$\mu_k(\mathbb{F}_\ell) = \{\zeta \in \mathbb{F}_\ell^* : \zeta^k = 1\} \qquad \text{and} \qquad A(k,\ell) = \{\zeta \in \mu_k(\mathbb{F}_\ell) : (4\zeta - 1/27) \in \mathbb{F}_\ell^2\}.$$

For each $\zeta \in A(k,\ell)$, let δ_ζ be some element of $\mathbb{F}_\ell$ satisfying $\delta_\zeta^2 = 4\zeta - 1/27$, and let

$$E_\zeta/\mathbb{F}_\ell : Y^2 = X^3 + \delta_\zeta X^2 + \zeta X.$$

Proposition 11.1. *Let $n \geq 17$ be a prime. Suppose there exists an integer k satisfying the following conditions:*

(a) *the integer $\ell = kn + 1$ is prime with $\ell \leq n^2/4$,*
(b) *$a_\ell(E) \neq \pm 2$,*
(c) *for all $\zeta \in A(k,\ell)$ we have $a_\ell(E_\zeta) \neq \pm a_\ell(E)$.*

Then equation (2) *does not have any non-trivial primitive solutions.*

Proof. Note first that $E_{a,b}$ and E respectively have the points $(a-b,0)$ and $(1,0)$ of order 2. Thus if ℓ is any odd prime of good reduction then $a_\ell(E_{a,b})$ and $a_\ell(E)$ are even.

Suppose now that ℓ satisfies the conditions of the proposition, and that equation (2) has a non-trivial primitive solution (a,b,c). We shall suppose first that $l \mid c$. In this case, Proposition 2.1 gives

$$\ell + 1 \equiv \pm a_\ell(E) \pmod{n}.$$

However, $\ell \equiv 1 \pmod{n}$ by assumption (a) of the proposition. Hence, $a_\ell(E) \equiv \pm 2 \pmod{n}$ and since $a_\ell(E)$ is even, $a_\ell(E) \equiv \pm 2 \pmod{2n}$. However, by the Hasse–Weil bounds and the assumption $\ell \leq n^2/4$ in (a) we have

$$|a_\ell(E) \mp 2| \leq 2\sqrt{\ell} + 2 \leq n + 2 < 2n.$$

This shows that $a_\ell(E) = \pm 2$, contradicting (b). We therefore deduce that ℓ does not divide $c = c_1 c_2$.

We shall now denote the reduction modulo ℓ map by $t \mapsto \overline{t}$. Recall (equation (3)) that ϵ and δ are related by $4\epsilon^n - 1/27 = \delta^2$. Moreover, $\epsilon = c_2/c_1^2$. Hence $(\overline{\epsilon^n})^k = \overline{1}$ and so $\overline{\epsilon^n} = \zeta$ for some $\zeta \in A(k,\ell)$. Clearly $\overline{\delta} = \pm\delta_\zeta$. Hence $E_\zeta/\mathbb{F}_\ell$ and $E_{\epsilon,\delta}/\mathbb{F}_\ell$ are quadratic twists, and so $a_\ell(E_\zeta) = \pm a_\ell(E_{\epsilon,\delta})$. However, $E_{\epsilon,\delta}$ is a quadratic twist of $E_{a,b}$, and by Proposition 2.1 we know that $a_\ell(E_{a,b}) \equiv a_\ell(E) \pmod{n}$. We deduce that $a_\ell(E_\zeta) \equiv \pm a_\ell(E) \pmod{n}$, and as both traces are even $a_\ell(E_\zeta) \equiv \pm a_\ell(E) \pmod{2n}$. Finally the assumption $\ell \leq n^2/4$ combined with the Hasse–Weil bounds shows that $a_\ell(E_\zeta) = \pm a_\ell(E)$, contradicting (c). This completes the proof. □

It remains to explain the difference between our Proposition 11.1 and Kraus' corresponding [23, Théorème 3.1]. Kraus in fact gives the same result with conditions (a), (b), (c) replaced by the following:

(a′) the integer $\ell = kn + 1$ is prime,
(b′) $a_\ell(E) \not\equiv \pm 2 \pmod{n}$,
(c′) for all $\zeta \in A(k,\ell)$ we have $a_\ell(E_\zeta) \not\equiv \pm a_\ell(E) \pmod{n}$.

To test condition (c′) we must compute $a_\ell(E)$ and $a_\ell(E_\zeta)$ for each $\zeta \in A(k,\ell)$. The set $A(k,\ell)$ can be somewhat large (it has an average size of about $k/2$), and for large ℓ this step is time consuming. However, condition (c) can be verified by computing $a_\ell(E)$ only: we simply choose a random point on E_ζ for each $\zeta \in A(k,\ell)$ and check that it is not annihilated by either of $\ell + 1 \pm a_\ell(E)$. If this holds then so does (c). In practice, for primes $n \approx 10^9$, we found that this brings a 10-fold speed up in the program run time.

12. Proof of Theorem 2

It is now clearly sufficient to prove that (2) has no non-trivial primitive solutions for prime exponents n in the range $10^4 < n < 10^9$. We wrote a simple program using the package `pari/gp` [1] to test whether a given prime n satisfies conditions (a), (b), (c) of Proposition 11.1, by finding a suitable integer k. Using this program we verified that (2) has no non-trivial primitive solutions for all prime exponents $10^4 < n < 10^9$. This computation took about 50 hours on a 2.8 GHz Dual-Core AMD Opteron.

References

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, *User's guide to PARI/GP*, `http://pari.math.u-bordeaux.fr/`

[2] M. Bennett, *On the equation* $x^{2n}+y^{2n} = z^5$, J. Théor. Nombres Bordeaux **18** (2006), 315–321.

[3] M. A. Bennett, J. S. Ellenberg and N. C. Ng, *The Diophantine equation* $A^4 + 2^\delta B^2 = C^n$, preprint.

[4] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54.

[5] F. Beukers, *The Diophantine equation* $Ax^p + By^q = Cz^r$, Lectures held at Institut Henri Poincaré, September 2004, `http://www.math.uu.nl/people/beukers/Fermatlectures.pdf`

[6] B. Birch and W. Kuyk, *Modular Functions of One Variable IV*, Lecture Notes in Math. **476**, Springer-Verlag, 1975.

[7] W. Bosma, J. Cannon and C. Playoust: *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://www.maths.usyd.edu.au/`)

[8] M. Bright and S. Siksek, *Functions, reciprocity and the obstruction to divisors on curves*, J. London Math. Soc. (2) **77** (2008), 789–807.

[9] J. W. S. Cassels, A. Fröhlich (Eds), *Algebraic Number Theory*, Academic Press, 1967.

[10] N. Bruin, *On powers as sums of two cubes*, pages 169–184 of *Algorithmic number theory* (edited by W. Bosma), Lecture Notes in Comput. Sci. **1838**, Springer, Berlin, 2000.

[11] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue–Nagell equation*, Compositio Math. **142** (2006), 31–62.

[12] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge University Press, 1997.

[13] H. Cohen, *Number Theory II. Analytic and Modern Methods*, GTM, Springer-Verlag, 2007.

[14] S. R. Dahmen, *Classical and modular methods applied to Diophantine equations*, University of Utrecht Ph.D. thesis, 2008.

[15] H. Darmon, *Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation*, C. R. Math. Rep. Acad. Sci. Canada **19** (1997), no. 1, 3–14.

[16] H. Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's Last Theorem*, Duke Math. J. **102** (2000), 413–449.

[17] H. Darmon and A. Granville, *On the Equation* $z^m = F(x,y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Society, **27** (1995), no. 6, 513–543.

[18] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. reine angew. Math. **490** (1997), 81–100.

[19] J. Edwards, *A complete solution to* $X^2 + Y^3 + Z^5 = 0$, J. reine angew. Math. **571** (2004), 213–236.

[20] J. 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.
[21] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Translated from the German by G. U. Brauer, J. R. Goldman and R. Kotzen, GTM **77**, Springer–Verlag, New York–Berlin, 1981.
[22] W. Ivorra and A. Kraus, *Quelques résultats sur les équations $ax^p + by^p = cz^2$*, Canad. J. Math. 58 (2006), no. 1, 115–153.
[23] A. Kraus, *Sur l'équation $a^3 + b^3 = c^p$*, Experimental Math. **7** (1998), 1–13.
[24] A. Kraus, *On the Equation $x^p + y^q = z^r$: A Survey*, Ramanujan Journal **3** (1999), 315–333.
[25] I. Niven, *The asymptotic density of sequences*, Bull. Amer. Math. Soc. **57** (1951), 420–434.
[26] B. Poonen, E. F. Schaefer, and M. Stoll, *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$*, Duke Math. J. **137** (2007), no. 1, 103–158.
[27] S. Siksek, *Sieving for rational points on hyperelliptic curves*, Math. Comp. **70** (2001), no. 236, 1661–1674.
[28] S. Siksek, *Descent on Picard groups using functions on curves*, Bull. Austral. Math. Soc. **66** (2002), 119–124.
[29] S. Siksek, *The modular approach to Diophantine equations*, notes for lectures delivered at the Institut Henri Poincaré (October 2004), `http://www.warwick.ac.uk/staff/S.Siksek/`.
[30] R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.
[31] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.

Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby, British Columbia, V5A 1S6, CANADA
E-mail address: `ichen@math.sfu.ca`

Samir Siksek, Institute of Mathematics, University of Warwick, Coventry, CV4 7AL, United Kingdom
E-mail address: `s.siksek@warwick.ac.uk`