The Fermat equation over $\mathbb{Q}(\sqrt{2})$

Frazer Jarvis and Paul Meekin*

Department of Pure Mathematics, University of Sheffield,
Sheffield S3 7RH, U.K.
a.f.jarvis@shef.ac.uk pmp99pm@shef.ac.uk
tel. 00441142223845, fax: 00441142223769

*The authors would like to thank GCHQ, Cheltenham, and the EPSRC for funding a CASE award.

Abstract

We study solutions of the Fermat equation defined over $\mathbb{Q}(\sqrt{2})$, and prove a version of 'Fermat's Last Theorem' over $\mathbb{Q}(\sqrt{2})$, assuming an unpublished result of Fujiwara.

AMS Subject Classification: 11D41; 11F41, 11F80

1 Introduction

As is well-known, one has the theorem ([28], [35], [39]):

Theorem 1.1 (Wiles,Taylor-Wiles) *The equation $x^n+y^n = z^n$ with $x, y, z \in \mathbb{Z}$ has no solutions with $xyz \neq 0$ when $n \geq 3$.*

The method of proof of this theorem, originating in Serre ([30]), also applies to some other Diophantine equations. However, there are other ways to generalise the theorem, and in this paper we will study solutions of the Fermat equation in $\mathbb{Q}(\sqrt{2})$, explaining that all the ideas of Ribet and Wiles carry through. There has been little study of Diophantine equations over more general number fields, and, as far as we are aware, no attempt has previously been made to apply Wiles's techniques to Diophantine problems over other fields. However, Hao and Parry [14] have generalised Kummer's approach to the Fermat equation using the arithmetic of cyclotomic extensions of quadratic fields.

Work of Debarre and Klassen [6] suggests the following conjecture:

Conjecture 1.2 (Debarre-Klassen) *Let K be a number field of degree d over $\mathbb{Q}$. Then the equation $x^n + y^n = z^n$ has only trivial solutions over K when $n \geq d + 2$.*

Here, Debarre and Klassen define *trivial solutions* to mean points (a, b, c) on $x^n + y^n = z^n$ where $a + b = c$. This deals not only with the rational points, but also with solutions such as $\omega^n + \overline{\omega}^n = 1$ when ω is a primitive 6th root of unity, belonging to any field containing $\mathbb{Q}(\sqrt{-3})$, and $n \equiv 1$ or $5 \pmod 6$.

In generalising the approach of Ribet and Wiles to a number field K, we need to have some notion of level lowering for modular forms over K. This means that, at present, we are restricted to totally real number fields, when we may use results for Hilbert modular forms similar to those of Ribet. The simplest case is that of a real quadratic number field. We indicate in this paper that all the numerology required to generalise the work of Ribet and Wiles directly continues to hold for $\mathbb{Q}(\sqrt{2})$. In the final part of the paper, however, we will explain that there are no other real quadratic fields for

which this is true, although some of the obstacles may be easy to overcome in some cases of small discriminant.

We shall prove the following theorem, which is a special case of the Debarre-Klassen conjecture.

Theorem 1.3 *The equation $x^n + y^n = z^n$ with $x, y, z \in \mathbb{Z}[\sqrt{2}]$ has no solutions with $xyz \neq 0$ when $n \geq 4$.*

We should stress that this result partly depends on Fujiwara's work ([11]) on level lowering, which remains unpublished. (Alternative published references are available for all but the proof of Mazur's Principle in even degree.)

The paper begins with a general discussion of solutions of the Fermat cubic over quadratic fields. In particular, the points on the Fermat cubic over $\mathbb{Q}(\sqrt{2})$ will be classified. The following section will concentrate on other small exponents. After this, we will begin the study of the Ribet-Wiles approach over $\mathbb{Q}(\sqrt{2})$, and prove Theorem 1.3 for prime exponents at least 17. Next, we will show that the method can be extended to prove the result for prime exponents at least 11. Finally, we consider the remaining small exponents (for which there are already results in the literature) to complete the proof of Theorem 1.3.

2 Exponent 3

In this section, we study the Fermat cubic over general quadratic fields. This has a long and distinguished history, notably through papers of Aigner, Fogels and Fueter, although their techniques were motivated by class field theory, rather than the theory of elliptic curves.

We prove the following elementary result, which completely classifies points on the Fermat cubic over real quadratic fields.

Lemma 2.1 *Solutions of $x^3+y^3 = 1$ over $\mathbb{Q}(\sqrt{d})$ are in correspondence with $\mathbb{Q}$-points on the elliptic curve $y^2 = x^3 - 432d^3$.*

Proof. One way to prove this is to use the fact that $x^3+y^3 = 1$ has only the rational points $(1, 0)$, $(0, 1)$ and the point at infinity (this is Fermat's Last Theorem for exponent 3 over $\mathbb{Q}$). If P denotes a point on the curve with coefficients in $\mathbb{Q}(\sqrt{d})$ but not in $\mathbb{Q}$, then P^σ is also on the curve, where σ denotes the non-trivial element in $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. The line joining P and P^σ is easily seen to have equation defined over $\mathbb{Q}$. Thus the three points of intersection of the line with the Fermat cubic are defined, as a set, over $\mathbb{Q}$. The element σ interchanges P and P^σ, so must fix the third point of intersection, R say. This point R is therefore a rational point on the Fermat

cubic, so is one of those listed above. Conversely, every line with rational slope passing through a rational point R on the Fermat cubic meets the cubic at two further points, and these are necessarily defined over a quadratic field.

We see that every point over a quadratic field on the Fermat cubic is the intersection of a rational line passing through a rational point. We can write down all such lines passing through $(1, 0)$ say; they are given by $y = a(x - 1)$ for $a \in \mathbb{Q}$. The x-coordinates of points of intersection of this line with the Fermat cubic are given by $x^3 + a^3(x - 1)^3 = 1$, which gives $(x - 1)(x^2 + x + 1 + a^3(x^2 - 2x + 1)) = 0$, so that the other x-coordinates are the roots of $(a^3 + 1)x^2 + (1 - 2a^3)x + (a^3 + 1) = 0$. Thus the points of intersection lie in $\mathbb{Q}(\sqrt{-12a^3 - 3})$, and this equals $\mathbb{Q}(\sqrt{d})$ if and only if $b^2 d = -12a^3 - 3$ for some $b \in \mathbb{Q}$. Thus we are searching for $\mathbb{Q}$-points on the elliptic curve $dy^2 = -12x^3 - 3$; it is easy to see that this is isomorphic to the Mordell curve $y^2 = x^3 - 432d^3$. □

Alternatively, it is easy to construct a proof from the observation that the Fermat cubic is isomorphic to $y^2 = x^3 - 432$, and the elliptic curve in the lemma is its quadratic twist over $\mathbb{Q}(\sqrt{d})$.

In the case where $d = 2$, it follows that $\mathbb{Q}(\sqrt{2})$-points on the Fermat cubic are in bijection with $\mathbb{Q}$-points on $y^2 = x^3 - 3456$, whose minimal Weierstrass model is $y^2 = x^3 - 54$ (curve 1728A2 in [4]). This is an elliptic curve of rank 1 and no non-trivial torsion; the group of $\mathbb{Q}$-points is generated by the point $(7, 17)$. This corresponds to the solution

$$(18 + 17\sqrt{2})^3 + (18 - 17\sqrt{2})^3 = 42^3. \tag{1}$$

(Note that Aigner [2] has shown that any point on the Fermat cubic defined over a quadratic field $\mathbb{Q}(\sqrt{d})$ may be written in the form $(a + b\sqrt{d})^3 + (a - b\sqrt{d})^3 = c^3$ for some $a, b, c \in \mathbb{Q}$, after multiplying by constants and rearranging the equation; this result can also be derived from Lemma 2.1 – indeed, there is a common factor of $\sqrt{2}$ in equation (1).)

As $y^2 = x^3 - 54$ has rank 1 and is torsion-free, the group of solutions to the Fermat cubic over $\mathbb{Q}(\sqrt{2})$ is isomorphic to $\mathbb{Z}$. For example, the point $[2](7, 17)$ corresponds to the solution

$$(707472 + 276119\sqrt{2})^3 + (707472 - 276119\sqrt{2})^3 = 1106700^3.$$

Similar methods may be used to determine the $\mathbb{Q}(\sqrt{d})$-points on the Fermat cubic for any d; for example, if $d = 3$, there are no points on the Fermat cubic except the three trivial rational points.

3 Proof of Theorem 1.3 for prime exponents at least 17

The strategy for studying the points on the Fermat curve of prime degree is the same as that of Ribet [28] and Wiles [39]. Given a prime exponent p, and a solution $\alpha^p + \beta^p = \gamma^p$ with α, β and γ in $\mathbb{Q}(\sqrt{2})$, we form the Frey curve $\mathcal{F}$, defined by

$$y^2 = x(x - \alpha^p)(x + \beta^p).$$

We say that an elliptic curve over $\mathrm{F} = \mathbb{Q}(\sqrt{2})$ is *modular* if there is some Hilbert cuspidal eigenform of weight $(2, 2)$ over F whose ℓ-adic Galois representations coincide with those of the curve. For $p \geq 17$, we will explain that this curve cannot be modular, contradicting a result of [22], and thus proving Theorem 1.3 in this case.

We begin by proving that the Frey curve $\mathcal{F}$ is semistable for $p \geq 11$, at least after suitably manipulating α, β and γ.

Lemma 3.1 *Suppose that $p \geq 11$. Given a non-trivial solution to (α, β, γ) to $x^p + y^p = z^p$ over $\mathbb{Q}(\sqrt{2})$, there is an associated Frey curve with a semistable model.*

Proof. To prove this, we simply go through Tate's Algorithm (see [32]). We may assume that (α, β, γ) are pairwise coprime. Note that $\mathcal{O}_\mathrm{F} = \mathbb{Z}[\sqrt{2}]$ and $\mathcal{O}_\mathrm{F}/(\sqrt{2}) \cong \{0, 1\}$, from which we observe that precisely one of α, β, γ is congruent to 0 (mod $\sqrt{2}$). Without loss of generality, assume that $\beta \equiv 0 \pmod{\sqrt{2}}$. Then either $\alpha \equiv \gamma \equiv 1 \pmod 2$ or $\alpha \equiv \gamma \equiv 1 + \sqrt{2} \pmod 2$.

Let u denote the fundamental unit $1 + \sqrt{2} \in \mathcal{O}_\mathrm{F}^\times$. Observe that if $\alpha \equiv 1 + \sqrt{2} \pmod 2$ then $\alpha u \equiv 1 \pmod 2$. Thus, multiplying throughout by u reduces us to the first case $\alpha \equiv \gamma \equiv 1 \pmod 2$. Further multiplying by -1 if necessary, we may assume without loss of generality that $\alpha \equiv 3 \pmod 4$. One now readily checks Tate's algorithm ([32], IV9), and verifies that the Frey curve $\mathcal{F}$,

$$y^2 = x(x - \alpha^p)(x + \beta^p)$$

over $\mathbb{Q}(\sqrt{2})$, has a semistable model. □

Next, we recall a result of Kraus ([24]):

Theorem 3.2 (Kraus) *Let K be a quadratic field whose ring of integers in principal, and let E be a semistable elliptic curve defined over K. Then if $E(\overline{K})$ contains a subgroup of order p stable under $\mathrm{Gal}(\overline{K}/K)$, then either $p \leq 13$ or $p | D_K N_{K/\mathbb{Q}}(u^2 - 1)$, where D_K denotes the discriminant of K, and u denotes the fundamental unit.*

Note that if $\mathrm{F} = \mathbb{Q}(\sqrt{2})$, $D_{\mathrm{F}} = 8$ and $N_{\mathrm{F}/\mathbb{Q}}(u^2 - 1) = -4$. If $p \geq 17$, we deduce that the mod p representation $\overline{\rho} = \overline{\rho}_{\mathcal{F},p}$ is absolutely irreducible.

Note also that the Frey curve has discriminant $16(\alpha\beta\gamma)^{2p}$, so that the mod p representation $\overline{\rho}$ is unramified at all primes except those above 2 and p, and is finite at primes above p. Since the Frey curve is semistable, no prime divides the conductor to a power greater than 1.

We also recall Theorem 9.6 of [22]:

Theorem 3.3 (Jarvis-Manoharmayum) *Every semistable elliptic curve over $\mathbb{Q}(\sqrt{2})$ is modular.*

This means that the p-adic Galois representation $\rho_{\mathcal{F},p}$ is isomorphic to $\rho_{f,p}$, the p-adic Galois representation associated to some modular form f of weight $(2,2)$ and some level. In particular, its reduction $\overline{\rho}$ is modular.

Since $\overline{\rho}$ is absolutely irreducible (remember that we are assuming that $p \geq 17$), we may now apply the main results of level lowering. Firstly, we add an auxiliary prime to the level, as in [34]. This allows us to use level lowering results whose proofs require geometric arguments on Shimura curves on quaternion algebras ramified at exactly one infinite place (and also at the auxiliary prime we have added). Using these results, we may remove all the primes from the level at which $\overline{\rho}$ is unramified, namely all those primes except those dividing 2 and p (and the auxiliary prime), using the main result of Rajaei's paper [27].

We may now remove the primes above p using the main result of [21] (working still with Shimura curves on this quaternion algebra), and finally remove the auxiliary prime using Fujiwara's version of Mazur's Principle for even degree ([11]). The only prime that remains is the prime $(\sqrt{2})$ above 2. Since the Frey curve is semistable, this prime can only occur with exponent at most 1 in the conductor of the Frey curve, and we conclude that $\overline{\rho}$ is modular of weight $(2,2)$ on the group

$$U_0(\sqrt{2}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \prod_{\mathfrak{q}} \mathrm{GL}_2(\mathcal{O}_{\mathrm{F},\mathfrak{q}}) \;\middle|\; \sqrt{2}|\gamma \right\}.$$

The definition of modular forms on these open compact subgroups are given in [15], (2.3). Since $\det U_0(\sqrt{2})$ is maximal, and since the strict class number of $\mathbb{Q}(\sqrt{2})$ is 1, these adelic modular forms coincide with the classical Hilbert cusp forms on the group

$$\Gamma_0(\sqrt{2}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}[\sqrt{2}]) \;\middle|\; \sqrt{2}|\gamma \right\}$$

using the isomorphism between adelic and classical modular forms given in [15], (2.6a).

Finally, we prove that there are no Hilbert cusp forms on this group. We compute the dimension of the space of cusp forms from the formula:

$$1 + \dim S_{(2,2)}(\Gamma) = \mathrm{vol}(\mathfrak{h}^2/\Gamma) + \sum_a E(\Gamma, a) + \sum_\kappa L(\Gamma, \kappa)$$

of Freitag ([10], II Theorem 4.8). Here, the volume term can be related to the value of a zeta function, and the contributions $E(\Gamma, a)$ (resp. $L(\Gamma, \kappa)$) of elliptic points a (resp. cusps κ) can also be made explicit in terms of various class numbers.

Since $\Gamma_0(\sqrt{2})$ is a subgroup of index 3 in $\mathrm{SL}_2(\mathbb{Z}[\sqrt{2}])$, and tables show that $\mathrm{vol}(\mathfrak{h}^2/\Gamma)$ is $\frac{1}{24}$, we see that $\mathrm{vol}(\mathfrak{h}^2/\Gamma_0(\sqrt{2})) = \frac{1}{8}$. The elliptic points of the full Hilbert modular group $\mathrm{SL}_2(\mathbb{Z}[\sqrt{2}])$ were computed by Gundlach ([13]), and one can use this to find the elliptic points for the subgroup. Some slight care must be taken here, as there are elliptc points of order 2 for the subgroup which lie above elliptic points of order 4 for the full modular group. We find that there are four elliptic points of order 2, each contributing $\frac{1}{8}$ to the formula, and two elliptic points of order 4, one contributing $\frac{1}{16}$ and the other contributing $\frac{5}{16}$. Finally, the cusp contribution is trivial for the full Hilbert modular group, and one can deduce the same result for the subgroup. Inserting all terms into the formula, we now have

$$\dim\, S_{(2,2)}(\Gamma_0(\sqrt{2})) = \frac{1}{8} + 0 + \frac{7}{8} - 1 = 0$$

as required.

Alternatively, we can switch to the totally definite quaternion algebra of discriminant 1, and use results of Vignéras [38] (see the table on pp.154–155) to deduce this result.

We therefore have a contradiction, which proves Theorem 1.3 for prime exponents $p \geq 17$.

4 Exponents 11 and 13

In the proof above, the assumption that $p \geq 17$ is used at only one point; for all the remaining implications, $p \geq 11$ is sufficient. Although the points on the Fermat equation of degree 11 over $\mathbb{Q}(\sqrt{2})$ are already known for $\mathbb{Q}(\sqrt{2})$ (and indeed over any field of degree at most 5 over $\mathbb{Q}$) by the work of Gross-Rohrlich [12], we shall give another proof here to motivate the case of exponent 13.

The requirement that $p \geq 17$ came from Kraus's paper [24] on the irreducibility of mod ℓ Galois representations associated to elliptic curves over $\mathbb{Q}(\sqrt{2})$. This may be best possible for general elliptic curves over $\mathbb{Q}(\sqrt{2})$, but the Frey curve has the additional property that its 2-torsion points are all defined over $\mathbb{Q}(\sqrt{2})$. In this section we shall indicate why such curves cannot have reducible mod 11 or mod 13 representations.

To give an elliptic curve whose 2-torsion is defined over $\mathbb{Q}(\sqrt{2})$, and which has a $\mathbb{Q}(\sqrt{2})$-rational subgroup of order p is equivalent to giving a non-cuspidal point on the modular curve X associated to the group $\Gamma(2) \cap \Gamma_0(p)$. The complex points of X are in bijection with $\mathfrak{h}/\Gamma(2) \cap \Gamma_0(p)$. The groups $\Gamma(2) \cap \Gamma_0(p)$ and $\Gamma_0(4p)$ are conjugate via the matrix $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. This gives an isomorphism from X to the curve $X_0(4p)$ defined on complex points by $z \mapsto 2z$. Both X and $X_0(4p)$ are defined over $\mathbb{Q}$ and the isomorphism between them is also defined over $\mathbb{Q}$. Thus the $\mathbb{Q}(\sqrt{2})$-points on X are in bijection with the $\mathbb{Q}(\sqrt{2})$-points on $X_0(4p)$.

Theorem 4.1 *There are no non-cuspidal $\mathbb{Q}(\sqrt{2})$-points on $X_0(44)$.*

Proof. There is a covering from the modular curve $X_0(44)$ to the elliptic curve

$$E \qquad y^2 = x^3 + x^2 + 3x - 1,$$

numbered 44A1 in Cremona's tables [4], and the degree of the modular parametrisation is 2. Furthermore, E has 3 rational points. However, E has no further $\mathbb{Q}(\sqrt{2})$-points, because if P were a $\mathbb{Q}(\sqrt{2})$-point on E, then $P \ominus P^\sigma$ would be a point $(a, b\sqrt{2})$ on E with $a, b \in \mathbb{Q}$. Then (a, b) would be a $\mathbb{Q}$-point on the quadratic twist of E to $\mathbb{Q}(\sqrt{2})$, which is the curve

$$E_2 \qquad y^2 = x^3 - x^2 + 11x - 19,$$

which is curve 704D1 in [4]. However, E_2 has no non-trivial $\mathbb{Q}$-points, so $P = P^\sigma$, and therefore P is a $\mathbb{Q}$-point on E. Thus there are exactly 3 $\mathbb{Q}(\sqrt{2})$-points on E, and therefore at most 6 $\mathbb{Q}(\sqrt{2})$-points on $X_0(44)$. But it is well known (see [26], for example) that if p is an odd prime, then $X_0(4p)$ has exactly 6 cusps, and all such cusps are rational. Therefore these are exactly all the $\mathbb{Q}(\sqrt{2})$-points on $X_0(44)$, which completes the proof of the theorem. □

Theorem 4.2 *There are no non-cuspidal $\mathbb{Q}(\sqrt{2})$-points on $X_0(52)$.*

Proof. We prove this in the same way as Theorem 4.1. The curve

$$E' \qquad y^2 = x^3 + x - 10,$$

labelled 52A1 in Cremona's tables [4], has 2 rational points, $(2,0)$ and $\mathcal{O}$, and admits a degree 3 modular parametrisation from $X_0(52)$. As before, let P denote a $\mathbb{Q}(\sqrt{2})$-point on E'; then $P \ominus P^\sigma$ corresponds to a point on the quadratic twist

$$E_2' \qquad y^2 = x^3 + 4x - 80,$$

which is curve 832D2 in [4]. This has 2 rational points, so we cannot immediately deduce the theorem in this case.

We first observe that the rank of 52A1 over $\mathbb{Q}(\sqrt{2})$ is the sum of its rank over $\mathbb{Q}$, and the rank over $\mathbb{Q}$ of its quadratic twist 832D2, which gives 0. Thus all $\mathbb{Q}(\sqrt{2})$ points are torsion, and we can compute the torsion group over $\mathbb{Q}(\sqrt{2})$ as in [31], § VII3. As the primes 7 and 17 split, $\mathbb{Q}(\sqrt{2})$ has residue fields (isomorphic to) $\mathbb{F}_7$ and $\mathbb{F}_{17}$. However, the curve has 10 points defined over $\mathbb{F}_7$ and 12 points defined over $\mathbb{F}_{17}$. In particular, there are no 17-torsion points (as (10,17)=1) or 7-torsion points (as (12,7)=1), and we conclude that the order of the torsion group therefore divides 10 and 12, and therefore has at most 2 elements, which must be the $\mathbb{Q}$-points on 52A1. $\square$

Corollary 4.3 *The mod 11 and mod 13 Galois representations associated to the Frey curve are irreducible.*

We see that the proof of Theorem 1.3 is also valid for $p = 11$ and $p = 13$.

5 Small exponents

To prove Theorem 1.3 for all exponents $n \geq 4$, we have to consider the cases $n = 4, 6, 9$, and prime exponents at least 5. Since we have dealt with prime exponents at least 11, it remains to consider the cases of exponents 4, 5, 6, 7 and 9.

All these cases are already considered in the literature (as is the case of exponent 11), although we give a new proof for exponent 6 below.

Exponent 4 was first proven by Aigner [1]; a stronger result classifying solutions of the Fermat quartic over all quadratic and cubic extensions of $\mathbb{Q}$ was obtained by Faddeev [8], and independently also by Mordell [25]. The only points in quadratic fields are defined over $\mathbb{Q}(\sqrt{-1})$ (solutions such as $i^4+0^4 = 1^4$) and over $\mathbb{Q}(\sqrt{-7})$ (the solutions are given by $x = \frac{1}{2}\epsilon_1(1+\epsilon\sqrt{-7})$, $y = \frac{1}{2}\epsilon_2(1-\epsilon\sqrt{-7})$, $z = 1$, and multiples of these, where ϵ, ϵ_1 and ϵ_2 are each ± 1). In particular, there are no non-trivial points over $\mathbb{Q}(\sqrt{2})$. Incidentally, the non-trivial solutions are all obtained as the points of intersection of the Fermat quartic with a line passing through two of the four rational points on the quartic $x^4 + y^4 = 1$ (a case of a stronger conjecture of [6])

Exponents 5 and 7 (and also exponent 11) were considered by Gross and Rohrlich [12]. The most complete result for exponent 5 was given by Klassen and Tzermias [23], in which all points on the Fermat quintic are classified which lie in extensions of $\mathbb{Q}$ of degree at most 6. Other than the three rational points on the Fermat quintic, there are only two solutions in quadratic fields, given by $(1\pm\sqrt{-3})^5+(1\mp\sqrt{-3})^5=2^5$, coming from the sixth roots of unity. Again, there are no non-trivial points over $\mathbb{Q}(\sqrt{2})$. Exponent 7 was also treated by Tzermias [36] in a similar way to the exponent 5 case. Tzermias classifies all points on the Fermat equation of degree 7 lying in an extension of $\mathbb{Q}$ of degree at most 5 (Gross and Rohrlich consider extensions of degree at most 3). Again, the only two solutions in quadratic fields, other than the three rational points, are $(1\pm\sqrt{-3})^7+(1\mp\sqrt{-3})^7=2^7$ and multiples of these. Therefore there are no non-trivial points over $\mathbb{Q}(\sqrt{2})$.

These proofs rely on the fact that the Jacobians of the Fermat curves of degree 5 and 7 have finitely many rational points. This is false for degree 6, and also for prime degree at least 11 ([9], [12]).

The cases of exponents 6 and 9 are also due to Aigner [3]; Aigner shows that the Fermat curves of degree 6 and 9 have no points over quadratic fields except the trivial rational points. Aigner's proof relies on an analysis of his standard form for solutions to $x^3+y^3=z^3$ mentioned above.

We give another proof for exponent 6 over $\mathbb{Q}(\sqrt{2})$ which is shorter and easier than Aigner's proof, although our proof will not generalise to every quadratic field. We first give a simple proof of Fermat's Last Theorem for exponent 6 over $\mathbb{Q}$ which makes no reference to exponent 3, and then explain that it generalises to $\mathbb{Q}(\sqrt{2})$.

Lemma 5.1 *Suppose that $a^6+b^6=c^6$ with $a,b,c\in\mathbb{Z}$. Then $abc=0$.*

Proof. Without loss of generality, we may assume that a, b and c are pairwise coprime. Then (a^3,b^3,c^3) form a Pythagorean triple, so that there exist non-zero coprime integers m and n such that

$$\begin{aligned} a^3 &= 2mn \\ b^3 &= m^2-n^2 \\ c^3 &= m^2+n^2. \end{aligned}$$

Multiply these together to get

$$(abc)^3=2m^5n-2mn^5.$$

Divide by n^6, put $u=\frac{m}{n}$ and $v=\frac{abc}{n^2}$ to get

$$v^3=2u^5-2u.$$

Multiply throughout by u^3, and set $x = uv$, $y = u^4$. We obtain the curve

$$x^3 = 2y^2 - 2y.$$

This curve is (isomorphic to) curve 108A1 in Cremona's tables [4]. We find that it has rank 0, and 3 rational points. These three points are visibly $(0, 0)$, $(0, 1)$ and the point at infinity (which cannot occur as $n \neq 0$). In the first two cases, $x = 0$, so $uv = 0$, and it is easy to see that $v = 0$, and then $abc = 0$ as required. □

The classification of Pythagorean triples is merely an explicit isomorphism between the projective line $\mathbb{P}^1$ and the projective circle $x^2 + y^2 = z^2$ given by $[m : n] \mapsto [2mn : m^2 - n^2 : m^2 + n^2]$, and this isomorphism is valid over any field not of characteristic 2.

Theorem 5.2 *The equation $a^6 + b^6 = c^6$ has no non-trivial solutions over $\mathbb{Q}(\sqrt{2})$.*

Proof. We may suppose $a, b, c \in \mathbb{Z}[\sqrt{2}]$ are all positive and have no common factor. Then (a^3, b^3, c^3) is a point on the circle, and points are parametrised by $(2kmn, k(m^2 - n^2), k(m^2 + n^2))$ as above, where k, m and n are in $\mathbb{Q}(\sqrt{2})$. In the same way as in Lemma 5.1, we get a $\mathbb{Q}(\sqrt{2})$-point P on the elliptic curve 108A1. Then $P \ominus P^\sigma$ will correspond to a point on the quadratic twist 1728F1 of 108A1 to $\mathbb{Q}(\sqrt{2})$. But this curve has no non-trivial $\mathbb{Q}$-points, so that $P = P^\sigma$, and P must be defined over $\mathbb{Q}$. But we have already noted that the 3 rational points on 108A1 correspond to trivial solutions to the Fermat sextic. □

6 A variant

In his original work, Serre ([30], §4.3) also explains that the same method of proof he suggested for the Fermat equation, and subsequently done by Ribet and Wiles, would also work for certain variants of the form

$$x^p + y^p = L^a z^p,$$

where L is a prime taken from a finite list, $a \in \mathbb{Z}_{\geq 0}$, and the exponent p is a prime different from L and at least 11. In this section, we wish to point out that a similar result is available for the variant

$$x^p + y^p = \lambda^a z^p$$

over $\mathbb{Q}(\sqrt{2})$, where λ is one of the primes $3 \pm \sqrt{2}$ dividing 7, and $p \geq 17$. The method of proof is the same as that above.

We start by assuming that a solution exists,

$$\alpha^p + \beta^p = \lambda^a \gamma^p.$$

Then we form the Frey curve

$$y^2 = x(x - \alpha^p)(x + \beta^p).$$

Over $\mathbb{Q}(\sqrt{2})$, this curve has a semistable model (as $p \geq 11$) and its mod p representation has conductor $\sqrt{2}\lambda$. Kraus's result (as $p \geq 17$) tells us that the mod p representation is absolutely irreducible. Next, the result of Jarvis-Manoharmayum gives that the Frey curve is modular, and so, in particular, the mod p representation is modular. Now level lowering (again assuming Fujiwara's version of Mazur's Principle with $[\mathbb{F} : \mathbb{Q}]$ even) allows us to show that there is a cuspidal Hilbert modular form of weight $(2, 2)$, an eigenvector for the Hecke operators, and on the group $U_0(\sqrt{2}\lambda)$. Again we can use a calculation similar to that above, listing the elliptic points and cusps, to see that the space $S_{(2,2)}(U_0(\sqrt{2}\lambda)) = (0)$ for these λ (this calculation can again be bypassed by referring to the tables of Vignéras [38]). We therefore obtain a contradiction, as before.

These two values of λ are the only primes for which there are no non-zero cusp forms in $S_{(2,2)}(U_0(\sqrt{2}\lambda)$. Serre uses tables of modular forms (over $\mathbb{Q}$) to deduce similar results for variant equations over $\mathbb{Q}$, even when $S_2(\Gamma_0(2L)) \neq (0)$, by observing that the mod p representations associated to Frey curves have certain congruence properties (coming from the fact that the curves have rational 2-torsion subgroups), and observing that the tables contain no forms whose mod p representations have these congruence properties. One direction for future research might be to construct tables of Hilbert modular forms and to deduce similar variants to those of Serre. Of course, the same method would also apply to the Fermat equation itself, and might bypass some of the obstructions noted below, although the only other real quadratic field for which the modularity of semistable elliptic curves is proven in [22] is $\mathbb{Q}(\sqrt{17})$.

7 Other quadratic fields

It will be observed that we have restricted attention to $\mathbb{Q}(\sqrt{2})$ thus far. In this section, we will make some comments on the situation over other real quadratic fields. We will now work over a more general field $\mathbb{Q}(\sqrt{d})$, and consider the Frey curve E, given by

$$y^2 = x(x - \alpha^p)(x + \beta^p),$$

associated to a putative non-trivial point $\alpha^p + \beta^p = \gamma^p$ on the Fermat curve of degree $p \geq 5$. For the moment, we make three assumptions that we will check later. We will assume that

1. the curve is semistable;
2. $\overline{\rho} = \overline{\rho}_{E,p}$ is absolutely irreducible;
3. the curve is modular.

We shall explore these properties later. The curve has discriminant $16(\alpha\beta\gamma)^{2p}$. It follows that its minimal discriminant is, apart from primes dividing 2, a pth power. Results of Edixhoven [7] (see also [5], Proposition 2.12) now imply that $\overline{\rho}$ is unramified away from 2 and from p, and that it is finite at primes dividing p.

We have the following:

Theorem 7.1 *Suppose that the Frey curve E satisfies the properties above. Then there is an adelic Hilbert cusp form g of weight $(2,2)$ of squarefree level dividing (2) such that $\overline{\rho}_{g,p} \cong \overline{\rho}$.*

Proof. The argument is the same as above. Since E is modular, there is some Hilbert cuspidal eigenform f such that $\rho_{E,p} \cong \rho_{f,p}$. The level of f is the same as the conductor of E, which is squarefree since E is semistable. We may add an auxiliary prime $\mathfrak{q}$ to the level and switch to a quaternion algebra ramified at this auxiliary prime and at one infinite place. We may remove all primes not dividing $2p$ from the level using Rajaei ([27], Main Theorem 1) or Jarvis ([19], Theorem 11.3), depending whether the prime $\mathfrak{p}$ has $N(\mathfrak{p}) \equiv 1 \pmod{p}$ or not (see also [11] for an alternative derivation of parts of this result). The main result of [21] allows us to remove a prime dividing the characteristic of the representation, under certain circumstances; the representation must be finite at the prime (which will be valid), and also we will require that the ramification be less than $p-1$. Since we are considering quadratic fields in this paper, the ramification degree will satisfy $e \leq 2 < 4 \leq p-1$. In addition, there is a mild hypothesis if $[F(\mu_p) : F] = 2$ which will never be true in any of the examples we consider at the end of the argument. We can therefore remove the primes dividing p, to leave ourselves with a form on the quaternion algebra of level dividing 2. Switching back to GL_2, we find a form of level dividing $2\mathfrak{q}$; the main result of Fujiwara's manuscript ([11]) allows us to remove this auxiliary prime. We conclude that $\overline{\rho}$ is modular of level dividing 2. Since E is semistable, it has squarefree conductor; apart from the auxiliary prime which we add (and then take

away), we do not increase the level, and so $\overline{\rho}$ is modular of squarefree level dividing (2). $\square$

For fields in which (2) is unramified, we will want to show that there are no forms of weight $(2,2)$ on $\Gamma_0(2)$. If $(2) = \mathfrak{p}^2$, we will want to prove the same result for forms of weight $(2,2)$ on $\Gamma_0(\mathfrak{p})$. For example, if $F = \mathbb{Q}(\sqrt{3})$, then $(2) = (\sqrt{3}+1)^2$, and so we should try to find an (adelic) Hilbert modular form of weight $(2,2)$ on the group $\Gamma_0((\sqrt{3}+1))$, and if $F = \mathbb{Q}(\sqrt{5})$, we want an adelic form of weight $(2,2)$ on the group $\Gamma_0(2)$.

We will begin by listing the fields for which this space is trivial: Hirzebruch, van der Ven and Zagier ([16], [17], [18]) prove that the complete list of fields for which there are no classical Hilbert modular forms (i.e., for which the genus of the corresponding Hilbert modular surface is zero) are those $\mathbb{Q}(\sqrt{d})$ with $d = 2$, 3, 5, 6, 7, 13, 15, 17, 21 and 33. A rather tedious case-by-case study of the cusps and elliptic points gives the following:

Theorem 7.2 *Let Γ_2 denote the classical subgroup of $\mathrm{SL}_2(\mathcal{O}_F)$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where c belongs to every prime ideal dividing (2). The genus of the Hilbert modular surface $\mathfrak{h}^2/\Gamma_2$ is zero if and only if $F = \mathbb{Q}(\sqrt{d})$ for $d = 2$, 3, 5 or 7.*

However, although the adelic modular forms are closely related to these classical forms, they only coincide when the narrow class number is 1. Indeed, it is known that there are elliptic curves with good reduction everywhere over $\mathbb{Q}(\sqrt{7})$, and these should correspond to adelic modular forms of level 1. The tables at the end of Vignéras ([38]) confirm that there are no adelic modular forms of the appropriate level for $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\sqrt{5})$, and these are the only real quadratic fields with this property.

This immediately implies that these are the only three fields which we need consider. We can check assumptions (1) and (2) above:

1. The Frey curve can always be made semistable over $\mathbb{Q}(\sqrt{2})$, at least if $p \geq 11$; over $\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\sqrt{5})$, this is not the case, and congruence conditions are required on α, β and γ to guarantee semistability. For $\mathbb{Q}(\sqrt{3})$, the result is:

   > Permute α, β and γ to assume that β is divisible by $\sqrt{3}+1$ (since the residue field is $\mathbb{F}_2$, this can be done). Then if $p \geq 11$, then the curve is semistable if and only if α is congruent modulo 4 to 1, 3, $2+\sqrt{3}$ or $2+3\sqrt{3}$.

   For $\mathbb{Q}(\sqrt{5})$, there is a similar conditional result:

The Frey curve is semistable if one of α, β and γ is divisible by 2 (this is not automatic, since the residue field is $\mathbb{F}_4$) and if $p \geq 5$.

2. Kraus's result again implies that if the Frey curve has a semistable model, then the mod p representation is absolutely irreducible if $p \geq 17$, since both fields have class number 1.

   Thus the first two assumptions hold under the given congruence conditions when $p \geq 17$.

3. The modularity results, however, tend to require a study of the mod 3 (or sometimes mod 5) representations associated to the curve, and many of these results require that 3 (or 5) is unramified is the quadratic field. Modularity results for fields in which 3 or 5 ramifies are likely to be difficult, and little is known currently. The first author intends to carry out further work into this problem, in collaboration with Jayanta Manoharmayum.

We deduce that there is an implication that modularity of semistable elliptic curves over $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$ implies that Fermat curves of prime degree at least 17 have no points over $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$ satisfying certain congruence conditions. We should remark, however, that (as in Serre [30], §4.3), the existence of modular forms is not necessarily a bar to proving positive results, and we anticipate that the Ribet-Wiles method could be used fruitfully for several other fields ($\mathbb{Q}(\sqrt{17})$, for example, where the modularity is demonstrated in [22]), given suitable computations of the modular forms.

Acknowledgements

We thank Kevin Buzzard, John Cremona and Steven Galbraith for helpful remarks regarding some of the numerical calculations in this paper.

References

[1] A.Aigner, Über die Möglichkeit von $x^4 + y^4 = z^4$ in quadratischen Körpern, Jber. Deutsch. Math.-Verein. 43 (1934) 226–229

[2] A.Aigner, Weitere Ergebnisse über $x^3 + y^3 = z^3$ in quadratischen Körpern, Monatshefte Math. 56 (1952) 240–252

[3] A.Aigner, Die Unmöglichkeit von $x^6 + y^6 = z^6$ und $x^9 + y^9 = z^9$ in quadratischen Körpern, Monatshefte Math. 61 (1957) 147–150

[4] J.Cremona, Algorithms for Modular Elliptic Curves, 2nd. ed., Cambridge University Press, Cambridge, UK (1997)

[5] F.Diamond, H.Darmon, R.Taylor, Fermat's Last Theorem, in: J.Coates, S.-T.Yau (eds.), Elliptic Curves, Modular Forms and Fermat's Last Theorem (2nd ed.), International Press (1997)

[6] O.Debarre, M.Klassen, Points of low degree on smooth plane curves, J. reine Angew. Math. 446 (1994) 81–87

[7] B.Edixhoven, The weight in Serre's conjectures on modular forms, Invent. Math. 109 (1992) 563–594

[8] D.Faddeev, Group of divisor classes on the curve defined by the equation $x^4 + y^4 = 1$, Soviet Math. Dokl. 1 (1960) 1149–1151

[9] D.Faddeev, The group of divisor classes on some algebraic curves, Soviet Math. Dokl. 2 (1961) 67–69

[10] E.Freitag, Hilbert Modular Forms, Springer, Berlin (1990)

[11] K.Fujiwara, Level optimisation in the totally real case, preprint (1999)

[12] B.Gross, D.Rohrlich, Some results on the Mordell-Weil group of the Jacobian of the Fermat curve, Invent. Math. 44 (1978) 201–224

[13] K.Gundlach, Die Fixpunkte einiger Hilbertscher Modulgruppen, Math. Ann. 157 (1965) 369–390

[14] F.Hao, C.Parry, The Fermat equation over quadratic fields, J. Number Theory 19 (1984) 115–130

[15] H¿Hida, On p-adic Hecke algebras for GL_2 over totally real fields, Ann. Math. 128 (1988) 295–384

[16] F.Hirzebruch, Hilbert modular surfaces, Enseignement Math. 19 (1973) 183–281

[17] F.Hirzebruch, A,van der Ven, Hilbert modular surfaces and the classification of algebraic surfaces, Invent. Math. 23 (1974) 1–29

[18] F.Hirzebruch, D.Zagier, Classification of Hilbert modular surfaces, in: Complex Analysis and Algebraic Geometry, CUP/Iwanami Shoten (1977) 43–77

[19] F.Jarvis, Mazur's Principle for totally real fields of odd degree, Compositio Math. 116 (1999) 39–79

[20] F.Jarvis, Level lowering for modular mod ℓ representations over totally real fields, Math. Ann. 313 (1999) 141–160

[21] F.Jarvis, Correspondences on Shimura curves and Mazur's Principle at p, Pacific J. Math. 213 (2004) 267–280

[22] F.Jarvis, J.Manoharmayum, On the modularity of elliptic curves over totally real fields, submitted (2003)

[23] M.Klassen, P.Tzermias, Algebraic points of low degree on the Fermat quintic, Acta Arith. 82 (1997) 393–401

[24] A.Kraus, Courbes elliptiques semi-stables et corps quadratiques, J. Number Theory 60 (1996) 245–253

[25] L.Mordell, The Diophantine equation $x^4 + y^4 = 1$ in algebraic number fields, Acta Arith. 14 (1967) 347–355

[26] A.Ogg, Rational points on certain elliptic modular curves, Proc. Symp. Pure Math. 24 (Analytic Number Theory, St Louis, 1972), American Mathematical Society, Providence, R.I. (1973) 221–231

[27] A.Rajaei, On the levels of mod ℓ Hilbert modular forms, J. reine angew. Math. 537 (2001) 33–65

[28] K.Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, Invent. Math. 100 (1990) 431–476

[29] J.-P.Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972) 259–331

[30] J.-P.Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math J. 54 (1987) 179–230

[31] J.Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics 106, Springer, New York (1986)

[32] J.Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics 151, Springer, New York (1994)

[33] C.Skinner, A.Wiles, Residually reducible representations and modular forms, Publ. Math. IHES 89 (1999) 5–126

[34] R.Taylor, Representations of Galois groups associated to Hilbert modular forms, in: L.Clozel, J.Milne (eds.), Automorphic Forms, Shimura Varieties and L-functions, vol.2, Academic Press, Boston (1990)

[35] R.Taylor, A.Wiles, Ring-theoretic properties of certain Hecke algebras, Ann. Math. 141 (1995) 553–572

[36] P.Tzermias, Algebraic points of low degree on the Fermat curve of degree seven, Manuscripta Math. 97 (1998) 483–488

[37] G.van der Geer, Hilbert modular surfaces, Ergebnisse der Mathematik und ihrer Grenzgebiete 16, Springer, Berlin (1988)

[38] M.-F.Vignéras, Arithmétique des algèbres de quaternions, Lecture Notes in Mathematics 800, Springer, Berlin (1980)

[39] A.Wiles, Modular elliptic curves and Fermat's Last Theorem, Ann. Math. 141 (1995) 443–551