ACTA ARITHMETICA
XCVIII.2 (2001)

Covering collections and a challenge problem of Serre

by

E. Victor Flynn (Liverpool) and
Joseph L. Wetherell (Los Angeles, CA)

1. Fermat quartics and Serre's challenge problem. The Fermat quartic curves $aX^4 + bY^4 = cZ^4$ and, in particular, the special cases

$$(1.1) \qquad \mathcal{D}: \quad X^4 + Y^4 = cZ^4,$$

for $c \in \mathbb{Z}$ not divisible by the fourth power of a prime, have been studied, for example, in [5], [13]. Local considerations tell us immediately that, if there are to be any non-trivial solutions (X, Y, Z) then any odd prime p dividing c must satisfy $p \equiv 1 \pmod 8$; furthermore $c \equiv 1, 2 \pmod{16}$, $c \not\equiv 3, 4 \pmod 5$, $c \not\equiv 7, 8, 11 \pmod{13}$, $c \not\equiv 4, 5, 6, 9, 13, 22, 28 \pmod{29}$. Indeed, these can be shown to be necessary and sufficient conditions for (1.1) to have solutions everywhere locally (note that there is a mistake on p. 67 of [13], where the condition (e) $c \not\equiv \pm 6, \pm 7 \pmod{17}$ should be deleted). This immediately excludes all values of $c \le 300$ except the eight values $c = 1, 2, 17, 82, 97, 146, 226, 257$. When local considerations do not immediately exclude a value of c, one can also make use of the maps $\phi_1 : (X, Y, Z) \mapsto (X^2, YZ, Z^2)$, $\phi_1' : (X, Y, Z) \mapsto (Y^2, XZ, Z^2)$ from $\mathcal{D}$ to the genus 1 curve $\mathcal{F}_1$, and the map $\phi_2 : (X, Y, Z) \mapsto (X^2, XY, Z^2)$ from $\mathcal{D}$ to the genus 1 curve $\mathcal{F}_2$, where

$$(1.2) \qquad \mathcal{F}_1: \quad X^2Z^2 + Y^4 = cZ^4, \qquad \mathcal{F}_2: \quad X^4 + Y^4 = cX^2Z^2,$$

which have respective Jacobians (see [13], p. 66, and [17]) given by the elliptic curves

$$(1.3) \quad \mathcal{E}_1: \quad V^2W = U^3 + 4cUW^2, \qquad \mathcal{E}_2: \quad V^2W = U^3 - (4/c^2)UW^2.$$

2000 *Mathematics Subject Classification*: Primary 11G30; Secondary 14H40.

The first author thanks the Nuffield Foundation (Grant SCI/180/96/71/G) for financial support.

The second author thanks the National Science Foundation (Grant DMS-9705959) for financial support.

If either $\mathcal{E}_1(\mathbb{Q})$ or $\mathcal{E}_2(\mathbb{Q})$ can be shown to have rank 0, then it is straightforward to determine all points in $\mathcal{D}(\mathbb{Q})$. For example, this easily allows the cases $c = 1, 2, 146, 226$ to be solved, leaving only $c = 17, 82, 97, 257$ (for $c \le 300$), where both elliptic curves have non-zero rank over $\mathbb{Q}$. Note that for all four of these cases there are obvious rational points on $\mathcal{D}$, for example: $(2, 1, 1), (3, 1, 1), (3, 2, 1), (4, 1, 1)$, respectively.

Another option is to try to use the method of Dem'yanenko (see [5], [13], pp. 62–66, and [15]), which is applicable when the curve $\mathcal{D}$ admits morphisms into some elliptic curve $\mathcal{E}$, and the rank of the group of morphisms $\mathcal{D} \to \mathcal{E}$ exceeds the rank of the Mordell–Weil group of $\mathcal{E}$ (the generalisation by Manin in [10], not relevant here, replaces the elliptic curve by any abelian variety). Dem'yanenko's method is effective, in the sense that if it is made explicit enough it will produce an upper bound for the heights of the rational points on the curve $\mathcal{D}$. In our case, ϕ_1 and ϕ_1' are independent maps from $\mathcal{D}$ to $\mathcal{E}_1$, and so the method of Dem'yanenko is applicable if $\mathcal{E}_1(\mathbb{Q})$ has rank 1. In fact, for all of $c = 17, 82, 97, 257$, $\mathcal{E}_1(\mathbb{Q})$ has rank 2, so that the method is not applicable. Serre asks ([13], p. 67) in particular whether the case $c = 17$ (the only unresolved $c \le 81$) has any solutions apart from the obvious ones: $(\pm 1, \pm 2, 1)$ and $(\pm 2, \pm 1, 1)$.

A further tool available is the following classical result of Chabauty [3].

Theorem 1.1. *Let $\mathcal{C}$ be a curve of genus g defined over a number field K, whose Jacobian has Mordell–Weil rank $\le g - 1$. Then $\mathcal{C}$ has only finitely many K-rational points.*

For all of $c = 17, 82, 97, 257$, the Jacobian of $\mathcal{D}$ has rank 6 over $\mathbb{Q}$, since it is isogenous over $\mathbb{Q}$ to $\mathcal{E}_1 \times \mathcal{E}_1 \times \mathcal{E}_2$, and $\mathcal{E}_1(\mathbb{Q}), \mathcal{E}_2(\mathbb{Q})$ both have rank 2. The genus of $\mathcal{D}$ is 3, and so Chabauty's theorem is not applicable.

A further failed attempt at Serre's question about $c = 17$ is described in [2], pp. 187–189, which looks at covers of $\mathcal{D}$. We briefly summarise here the algebra required to obtain the covers, and refer the reader to [2] for further details. First note that, when $c = 17$, the equation for $\mathcal{D}$ can be written

$$\begin{aligned}\{17Z^2 + (5X^2 - 4XY + 5Y^2)\}\{17Z^2 - (5X^2 - 4XY + 5Y^2)\}& \\ = -2(2X^2 - 5XY + 2Y^2)^2.&\end{aligned}\tag{1.4}$$

The two factors on the left hand side of (1.4) do not have any common zeros on $\mathcal{D}$. It follows that the double cover of $\mathcal{D}$ given by the pair of equations

$$\begin{aligned}17Z^2 + (5X^2 - 4XY + 5Y^2) &= dR^2,\\ dR^2\{17Z^2 - (5X^2 - 4XY + 5Y^2)\} &= -2(2X^2 - 5XY + 2Y^2)^2,\end{aligned}\tag{1.5}$$

is, in fact, an unramified cover for every choice of non-zero $d \in \mathbb{Z}$. Every rational point on $\mathcal{D}$ can be lifted to a rational point on (1.5) for some choice of d. On the other hand, the resultant of the two factors on the left hand side of (1.4) is 34, so (1.5) cannot have rational solutions unless d divides 34. We can cut this down even further using local considerations and automorphisms on $\mathcal{D}$.

Let (X, Y, Z) be a rational point on $\mathcal{D}$. We may take X, Y, Z to be coprime integers. Then $X \not\equiv 0$, $Y \not\equiv 0 \pmod{17}$ and, without loss of generality, $X \not\equiv 0,\ Y \equiv 0,\ Z \not\equiv 0 \pmod 2$. By taking $-Y$ for Y if need be, we may suppose that

$$2X^2 - 5XY + 2Y^2 = (2X - Y)(X - 2Y) \equiv 0 \pmod{17}. \tag{1.6}$$

It follows that the greatest common divisor of the two main factors on the left hand side of (1.4) is 34, and that $5X^2-4XY+5Y^2$ is positive and congruent to 1 modulo 4. This shows that, up to automorphism, every rational point on $\mathcal{D}$ comes from a rational point on (1.5) with $d = 34$. Incorporating the choice $d = 34$ and rewriting slightly, we obtain

$$\begin{aligned} 17Z^2 + (5X^2 - 4XY + 5Y^2) &= 34R^2, \\ 17Z^2 - (5X^2 - 4XY + 5Y^2) &= -68S^2, \\ 2X^2 - 5XY + 2Y^2 &= 34RS, \end{aligned} \tag{1.7}$$

for some integers R, S; that is,

$$\begin{aligned} (X + Y)^2 &= 9(R^2 + 2S^2) - 28RS, \\ (X - Y)^2 &= R^2 + 2S^2 + 12RS, \\ Z^2 &= R^2 - 2S^2. \end{aligned} \tag{1.8}$$

The equations (1.8) define a curve of genus 5, which covers the genus 2 curve

$$T^2S^4 = (9R^2 - 28RS + 18S^2)(R^2 + 12RS + 2S^2)(R^2 - 2S^2). \tag{1.9}$$

If we can show that the only rational points on (1.9) are those with $S = 0$ then we could deduce from $(2X - Y)(X - 2Y) = 34RS$, the third equation in (1.7), that the only points on $\mathcal{D}(\mathbb{Q})$ are the obvious ones, which would answer Serre's challenge. We write the genus 2 curve in affine form

$$\mathcal{C}: \quad y^2 = (9x^2 - 28x + 18)(x^2 + 12x + 2)(x^2 - 2). \tag{1.10}$$

It is sufficient to show that $\mathcal{C}(\mathbb{Q})$ contains no affine points, that is, to show that $\mathcal{C}(\mathbb{Q}) = \{\infty^+, \infty^-\}$, where by ∞^+, ∞^- we mean the points on the nonsingular curve that lie over the point at infinity on $\mathcal{C}$. It would be natural now to make another attempt at using Chabauty's theorem, and in particular the explicit techniques in [7], [8] which would apply if the Jacobian of $\mathcal{C}$ were to have rank 0 or 1 over $\mathbb{Q}$. However, as we shall see, the Jacobian has rank 2 over $\mathbb{Q}$, and so the problem just barely eludes this attack with the same efficiency as it eluded the method of Dem'yanenko.

In the next section we shall show that in order to find $\mathcal{C}(\mathbb{Q})$, it suffices to find a special set of solutions to an equation which describes a genus 1 curve defined over a quartic number field. In Section 3 we will find this special set of solutions. In this way we can show that $\mathcal{C}(\mathbb{Q}) = \{\infty^+, \infty^-\}$, thus proving that $X^4 + Y^4 = 17Z^4$ has only the known points. It will be clear that our techniques in the following sections, which build on those in [1], [4], [9], [18], give a method of attack not only for $\mathcal{C}$, but also for any hyperelliptic curve.

We suspect that a similar strategy will apply in principle to the other unresolved values of $c = 82, 97, 257, \ldots$, although we have not attempted this, as one needs to perform computations in $\mathbb{Q}(\sqrt{2}, \sqrt{c})$, which become time consuming as c increases.

2. From genus 2 to genus 1.

In this section we prove the following proposition.

Proposition 2.1. *Let $\mathcal{C}$ be the genus 2 curve defined over $\mathbb{Q}$ by*

$$\mathcal{C}: \quad y^2 = (9x^2 - 28x + 18)(x^2 + 12x + 2)(x^2 - 2), \tag{2.1}$$

and let $\mathcal{F}$ be the genus 1 curve defined over $K = \mathbb{Q}(\sqrt{2}, \sqrt{34})$ by

$$\mathcal{F}: \quad v^2 = (9x^2 - 28x + 18)(x - (-6 + \sqrt{34}))(x - \sqrt{2}). \tag{2.2}$$

If $x \in \mathbb{Q}$ is the x-coordinate for some affine point $(x, y) \in \mathcal{C}(\mathbb{Q})$, then it is also the x-coordinate for some affine point $(x, v) \in \mathcal{F}(K)$.

This proposition has the following implication. If the set of K-rational points on $\mathcal{F}$ which have x-coordinate in $\mathbb{Q}$ is finite, and if we can determine this set, then we can determine the set $\mathcal{C}(\mathbb{Q})$. In Section 3 we shall show how to satisfy both of these hypotheses.

Define $\{\alpha_1, \alpha_2\}$, $\{\beta_1, \beta_2\}$, $\{\gamma_1, \gamma_2\}$ to be the roots of $9x^2 - 28x + 18$, $x^2 + 12x + 2$, and $x^2 - 2$, respectively. We will need the following computational result.

Lemma 2.2. *Let $\mathcal{C}$ be the curve of genus 2 defined in Proposition 2.1, and let J be the Jacobian of $\mathcal{C}$. Then $J(\mathbb{Q}) \cong \mathbb{Z}^2 \times (\mathbb{Z}/2\mathbb{Z})^2$. The quotient group $J(\mathbb{Q})/2J(\mathbb{Q})$ is generated by the divisor classes*

$$\begin{aligned} T_1 &= [(\alpha_1, 0) - (\alpha_2, 0)], & T_2 &= [(\beta_1, 0) - (\beta_2, 0)], \\ D_1 &= [\infty^+ - \infty^-], & D_2 &= [(x_1, y_1) + (x_2, y_2) - \infty^+ - \infty^-], \end{aligned} \tag{2.3}$$

where x_1, x_2 are the roots of $5x^2 - 18x + 17$, and

$$y_j = 3(-603x_j + 1187)/50 \quad \text{for } j = 1, 2. \tag{2.4}$$

The divisor classes T_1 and T_2 are 2-torsion, while D_1 and D_2 have infinite order.

Proof. This result was obtained by a standard 2-descent using the technique first described in [11]. The details of the computation are in the file ftp://ftp.liv.ac.uk/pub/genus2/serrecurve/rank.computation. ■

Proof of Proposition 2.1. Let $F(x)$ be the right hand side of the equation for $\mathcal{F}$, that is, $F(x) = (9x^2 - 28x + 18)(x - (-6 + \sqrt{34}))(x - \sqrt{2})$. Consider $F(x)$ as a K-rational function on $\mathcal{C}$. The divisor of F is $2D$, where $D = (\alpha_1, 0) + (\alpha_2, 0) + (-6 + \sqrt{34}, 0) + (\sqrt{2}, 0) - 2\infty^+ - 2\infty^-$. Let $\mathrm{Div}_D\mathcal{C}(K)$ be the set of K-rational divisors on $\mathcal{C}$ whose support is disjoint from that of D. We define a homomorphism $q_F : \mathrm{Div}_D\mathcal{C}(K) \to K^*$ by

$$q_F\Big(\sum n_j P_j\Big) = \prod F(P_j)^{n_j}, \tag{2.5}$$

extended to all K-rational divisors by defining $q_F(\infty^+) = q_F(\infty^-) = 1$ and by the rule $q_F((\alpha, 0)) = (F(x)/(x - \alpha))(\alpha)$ if $F(\alpha) = 0$.

In fact, q_F induces a homomorphism $q_F : J(K)/2J(K) \to K^*/(K^*)^2$. This is an easy consequence of Weil reciprocity and the fact that the divisor of F is twice a K-rational divisor. See [12], [16] for details.

A short computation shows that

$$q_F(T_1) = q_F(T_2) = q_F(D_1) = q_F(D_2) = 1 \quad \text{in } K^*/(K^*)^2. \tag{2.6}$$

In particular, this means that if P is any $\mathbb{Q}$-rational point of $\mathcal{C}$, then $q_F(P) \in (K^*)^2$. If $P = (x, y)$ is a Q-rational affine point, then $F(x) \neq 0$, so $q_F(P) = F(x)$. We thus conclude that there is some $v \in K^*$ such that

$$v^2 = (9x^2 - 28x + 18)(x - (-6 + \sqrt{34}))(x - \sqrt{2}). \tag{2.7}$$

This is the equation for $\mathcal{F}$, so we have proven the proposition. ■

3. A Chabauty-like argument. In the introduction we showed that any unexpected point on the Serre $c = 17$ curve would give a $\mathbb{Q}$-rational affine point on the genus 2 curve $\mathcal{C}$, and in Section 2 we showed that any such point on $\mathcal{C}$ would produce a K-rational affine point on $\mathcal{F}$ with $\mathbb{Q}$-rational x-coordinate. In this section we show that no such point exists.

Proposition 3.1. *Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{34})$ and let $\mathcal{F}$ be the genus 1 curve defined over K by*

$$\mathcal{F}: \quad v^2 = (9x^2 - 28x + 18)(x - (-6 + \sqrt{34}))(x - \sqrt{2}). \tag{3.1}$$

There is no affine point $(x, v) \in \mathcal{F}(K)$ with $x \in \mathbb{Q}$.

The genus 1 curve $\mathcal{F}$ has two K-rational points at infinity, which we will call ∞^+ and ∞^-. To distinguish these points, we will let ∞^+ denote the point at which v/x^2 evaluates to 3. We consider $\mathcal{F}$ to be an elliptic curve with the point ∞^+ serving as the group identity.

Lemma 3.2. *$\mathcal{F}(K) = \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The point $P = (-6 + \sqrt{34}, 0)$ has infinite order and is not the double of any point in $\mathcal{F}(K)$.*

Proof. Standard 2-descent and reduction arguments, such as those described in [6], [14]. ∎

Proof of Proposition 3.1. We start with a brief overview of our strategy. Suppose that (x_0, v_0) is a K-rational affine point on $\mathcal{F}$ with $x_0 \in \mathbb{Q}$. Our first step is to show that x_0 must reduce to ∞ at both primes $\mathfrak{p}_1, \mathfrak{p}_2$ lying over $p = 7$. Focusing on the first prime, we see that (x_0, v_0) must be in the same residue class on $\mathcal{F}(K_{\mathfrak{p}_1})$ as either ∞^+ or ∞^-. It suffices to consider the residue class of ∞^+. This leads to a simple argument in the kernel of reduction of $\mathcal{F}(K_{\mathfrak{p}_1})$.

Now for the details. The two primes above 7 in K are

$$\mathfrak{p}_1 = (7, 3 - \sqrt{2}) \quad \text{and} \quad \mathfrak{p}_2 = (7, 3 + \sqrt{2}). \tag{3.2}$$

Both primes are unramified and have residue field $\mathbb{F}_{49} = \mathbb{F}_7(\sqrt{34})$. The curve $\mathcal{F}$ has good reduction at both primes. For clarity, we use k_1 and k_2 to denote the residue fields of $\mathfrak{p}_1$ and $\mathfrak{p}_2$, respectively.

Let $\mathcal{F}_1$, $\mathcal{F}_2$ denote the reduction of $\mathcal{F}$ at $\mathfrak{p}_1$, $\mathfrak{p}_2$, respectively. A quick count shows that $\mathcal{F}_1(k_1)$ has 36 points; we also find that 9 of these points are 3-torsion, so $\mathcal{F}_1(k_1) \cong (\mathbb{Z}/6\mathbb{Z})^2$. Similar computations show that $\mathcal{F}_2(k_2) \cong \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let P be the point of infinite order from Lemma 3.2. The reduction of P has order 3 in $\mathcal{F}_1(k_1)$ and order 13 in $\mathcal{F}_2(k_2)$. Thus, P is not in $3\mathcal{F}(K)$ or $13\mathcal{F}(K)$, and is not in $2\mathcal{F}(K)$ by Lemma 3.2.

Let G be the subgroup of $\mathcal{F}(K)$ generated by P and 2-torsion. We would like to say that $G = \mathcal{F}(K)$, but verifying this would require a long computation. Moreover, it is unnecessary, in that we have shown that both groups have the same image in $\mathcal{F}_1(k_1) \times \mathcal{F}_2(k_2)$. This image has size $4 \cdot 3 \cdot 13$ and is of index 12 in $\mathcal{F}_1(k_1) \times \mathcal{F}_2(k_2)$.

By assumption, $x_0 \in \mathbb{Q}$. We conclude that x_0 reduces to the same value at both primes, and that this value lies in $\mathbb{F}_7 \cup \{\infty\}$. We look for points in the reduction of $\mathcal{F}(K)$ that have this property. In other words, for each torsion point $T \in \mathcal{F}(K)[2]$ and each integer $0 \le n \le 38$ we compute the reduction of $T + [n]P$ in both $\mathcal{F}_1(k_1)$ and $\mathcal{F}_2(k_2)$. We find that the only times $x(T + [n]P)$ reduces to the same value in $\mathbb{F}_7 \cup \{\infty\}$ at both primes are when that value is ∞. We conclude that the denominator of x_0 must be divisible by 7.

We now restrict our attention to $\mathfrak{p}_1$. We change variables to $s = 1/x$ and $t = y/x^2$ and set $s_0 = 1/x_0$, $t_0 = y_0/x_0^2$. Then our equation for $\mathcal{F}$ becomes

$$\mathcal{F}: \quad t^2 = (18s^2 - 28s + 9)((-6 + \sqrt{34})s - 1)(\sqrt{2}\, s - 1), \tag{3.3}$$

and we are looking for a point $(s_0, t_0) \in \mathcal{F}(K)$ with $s_0 \in \mathbb{Q}$, $7 \mid s_0$, and

$s_0 \neq 0$. Replacing t_0 with $-t_0$ if necessary, we can assume that t_0 reduces to 3 modulo $\mathfrak{p}_1$.

Note that ∞^+ is written as $(0,3)$ in (s,t)-coordinates. The kernel of reduction is the set $\{(s,t) \in \mathcal{F}(K_{\mathfrak{p}_1}) : (s,t) \equiv (0,3) \pmod{7}\}$; equivalently, the kernel of reduction is the residue class of the group identity element.

Suppose (s,t) is in the kernel of reduction and write $s = 7^i s'$ with s' a unit in $\mathbb{Z}_{\mathfrak{p}_1}$. Since $\mathfrak{p}_1$ is unramified and $p > 2$, basic results about formal groups tell us that the s-coordinate of $[7^n m](s,t)$ is congruent to $7^{i+n} m s'$ modulo 7^{i+n+1}. We will call s' the *leading term* of the point (s,t); the previous statement shows that we can compute with leading terms, modulo 7.

We know that P has order 3 modulo $\mathfrak{p}_1$; thus, $[3]P$ is a non-trivial K-rational point in the kernel of reduction. We compute that

$$s([3]P) \equiv 7 \cdot (3 + 2\sqrt{34}) \pmod{7^2}. \tag{3.4}$$

Using the results in the previous paragraph and the fact that $\mathcal{F}(K)$ has rank 1, we see that either any K-rational point in the kernel of reduction is the identity or the leading term is an integer multiple of $3+2\sqrt{34}$ modulo 7. But the leading term of (s_0, t_0) is a non-zero rational number, hence it cannot involve $\sqrt{34}$. This is a contradiction.

If (s_0, t_0) cannot exist, then (x_0, v_0) cannot exist, either. It follows that there is no affine point $(x, v) \in F(K)$ with $x \in \mathbb{Q}$. This completes the proof of Proposition 3.1. ∎

4. Potential application to other Fermat quartics. The main interest of the above methods is that they are applicable to any hyperelliptic curve, with the solution of Serre's curve, via its associated genus 2 curve, being a fringe benefit. Nevertheless, we shall consider here whether such techniques do, in fact, give a method of attacking Fermat quartics for other unsolved values of c.

It seems, from looking at the current list of unsolved values for c, that the most usual difficult case for solving $X^4 + Y^4 = cZ^4$ is when, as for $c = 17$, there is a known $\mathbb{Q}$-rational point, and we wish to find all of them. It is natural to ask whether the genus 2 curve (1.10) is special to the case $c = 17$, or whether such a covering exists for general c. Consider the case when $c = p$, an odd prime, with $p = a^4 + b^4$ for $a, b \in \mathbb{Z}$. This includes the unsolved cases $c = 97, 257$. Equation (1.4) generalises to

$$(pZ^2 + \psi_1(X,Y))(pZ^2 - \psi_1(X,Y)) = -2\psi_2(X,Y)^2, \tag{4.1}$$

where

$$\psi_1(X,Y) = (a^2 + b^2)X^2 - 2abXY + (a^2 + b^2)Y^2,$$
$$\psi_2(X,Y) = abX^2 - (a^2 + b^2)XY + abY^2.$$

A straightforward imitation of the argument in the introduction gives that

$$\begin{aligned} pZ^2 + \psi_1(X,Y) &= 2pR^2, \\ pZ^2 - \psi_1(X,Y) &= -4pS^2, \\ \psi_2(X,Y) &= 2pRS, \end{aligned} \tag{4.2}$$

for some integers R, S; that is,

$$\begin{aligned} (X+Y)^2 &= (a+b)^2(R^2+2S^2) - 4(a^2+ab+b^2)RS, \\ (X-Y)^2 &= (a-b)^2(R^2+2S^2) + 4(a^2-ab+b^2)RS, \\ Z^2 &= R^2 - 2S^2. \end{aligned} \tag{4.3}$$

The equations (4.3) define a curve of genus 5, which covers the genus 2 curve, given in affine form as

$$\mathcal{C}: \quad y^2 = G_1(x)G_2(x)G_3(x), \tag{4.4}$$

where

$$\begin{aligned} G_1(x) &= (a+b)^2x^2 - 4(a^2+ab+b^2)x + 2(a+b)^2, \\ G_2(x) &= (a-b)^2x^2 + 4(a^2-ab+b^2)x + 2(a-b)^2, \\ G_3(x) &= x^2 - 2. \end{aligned} \tag{4.5}$$

As usual, in order to find all $\mathbb{Q}$-rational points on $X^4 + Y^4 = pZ^4$, it is sufficient to find those on $\mathcal{C}$ of (4.4). In particular, if $\mathcal{C}(\mathbb{Q})$ contains no affine points, then $(\pm a, \pm b, 1)$ are the only $\mathbb{Q}$-rational points on $X^4 + Y^4 = pZ^4$.

For $X^4 + Y^4 = cZ^4$, for a given composite value of c, a similar argument gives a finite set of curves of genus 2 and it is sufficient to find all $\mathbb{Q}$-rational points on them. Therefore, the methods of Sections 1–3 are indeed potentially applicable to such curves. For each of the currently unsolved values of c, with a known solution to $X^4 + Y^4 = cZ^4$, there will be corresponding elliptic curves over quartic number fields, similar to (2.7). We would then, in principle, have an attack on finding all solutions to $X^4 + Y^4 = cZ^4$, provided that all of our elliptic curves have rank less than 4. A computational restraint is the algebraic number theory involved in finding these ranks, which will typically be more demanding than in our example of Section 2, where we had the good luck that $\mathbb{Q}(\sqrt{34}, \sqrt{2})$ has class number 1.

References

[1] N. Bruin, *Chabauty methods and covering techniques applied to generalised Fermat equations*, PhD dissertation, Leiden, 1999.

[2] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge Univ. Press, 1996.

[3] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris 212 (1941), 882–885.

[4] K. R. Coombes and D. R. Grant, *On heterogeneous spaces*, J. London Math. Soc. (2) 40 (1989), 385–397.

[5] V. Dem'yanenko, *Rational points on a class of algebraic curves*, in: Amer. Math. Soc. Transl. 66, Amer. Math. Soc., Providence, RI, 1968, 246–272.

[6] Z. Djabri, E. F. Schaefer and N. P. Smart, *Computing the p-Selmer group of an elliptic curve*, Trans. Amer. Math. Soc. 352 (2000), 5583–5597.

[7] E. V. Flynn, *A flexible method for applying Chabauty's Theorem*, Compositio Math. 105 (1997), 79–94.

[8] E. V. Flynn, B. Poonen and E. F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-two curve*, Duke Math. J. 90 (1997), 435–463.

[9] E. V. Flynn and J. L. Wetherell, *Finding rational points on bielliptic genus 2 curves*, Manuscripta Math. 100 (1999), 519–533.

[10] Yu. Manin, *The p-torsion of elliptic curves is uniformly bounded*, Izv. Akad. Nauk SSSR 33 (1969), 459–465 (in Russian).

[11] E. F. Schaefer, *2-descent on the jacobians of hyperelliptic curves*, J. Number Theory 51 (1995), 219–232.

[12] —, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. 310 (1998), 447–471.

[13] J.-P. Serre, *Lectures on the Mordell–Weil Theorem*, transl. and ed. by Martin Brown, from notes by Michel Waldschmidt, Vieweg, 1989.

[14] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

[15] —, *Rational points on certain families of curves of genus at least* 2, Proc. London Math. Soc. (3) 55 (1987), 465–481.

[16] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith., to appear.

[17] A. Weil, *Remarques sur un mémoire d'Hermite*, Arch. Math. (Basel) 5 (1954), 197–202.

[18] J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, PhD dissertation, Univ. of California at Berkeley, 1997.

Department of Mathematical Sciences
University of Liverpool
Liverpool L69 3BX, United Kingdom
E-mail: evflynn@liv.ac.uk

Department of Mathematics
University of Southern California
Los Angeles, CA 90089-1113, U.S.A.
E-mail: jlwether@alum.mit.edu

Received on 9.5.2000
and in revised form on 3.8.2000 (3821)