APPLICATION OF COVERING TECHNIQUES TO FAMILIES OF CURVES

E.V. FLYNN AND J. REDMOND

Abstract. Much success in finding rational points on curves has been obtained by using Chabauty's Theorem, which applies when the genus of a curve is greater than the rank of the Mordell-Weil group of the Jacobian. When Chabauty's Theorem does not directly apply to a curve $\mathcal{C}$, a recent modification has been to cover the rational points on $\mathcal{C}$ by those on a covering collection of curves $\mathcal{D}_i$, obtained by pullbacks along an isogeny to the Jacobian; one then hopes that Chabauty's Theorem applies to each $\mathcal{D}_i$. So far, this latter technique has been applied to isolated examples. We apply, for the first time, certain covering techniques to infinite families of curves. We find an infinite family of curves to which Chabauty's Theorem is not applicable, but which can be solved using bielliptic covers, and other infinite families of curves which even resist solution by bielliptic covers. A fringe benefit is an infinite family of Abelian surfaces with non-trivial elements of the Tate-Shafarevich group killed by a bielliptic isogeny.

1. Introduction

The following result of Chabauty[6] gives a way of deducing information about the K-rational points on a curve from its Jacobian.

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

This is a weaker result than Faltings' Theorem; however, when applicable, Chabauty's method can often be used to give good bounds for the number of points on a curve. These ideas have been developed in [7], [8], [14], [15]. When the conditions of Theorem 1 are satisfied, local considerations give a bound on the order of $\mathcal{C}(K)$, which one hopes is attained by the known points. This has been applied to solve several naturally occurring problems, such as [9], where Chabauty's method is used to show that the curve

$$Y^2 = X^6 + 8X^5 + 22X^4 + 22X^3 + 5X^2 + 6X + 1 \tag{1}$$

has only the six rational points: $(0,1), (0,-1), (-3,1), (-3,-1), \infty^+, \infty^-$, where ∞^+, ∞^- denote the points on the non-singular curve that lie over the singular point at infinity. It follows from this (as described in [9]) that there is no quadratic polynomial $f(z)$ in $\mathbb{Q}[z]$ with a rational point of exact period 5 – that is to say, for which $f^5(z) = z$, but z is not equal to $f^i(z)$ for any $1 \leq i \leq 4$. The Jacobian $\mathcal{J}$ of the curve in (1) satisfies $\mathrm{rank}(\mathcal{J}(\mathbb{Q})) = 1$, and so Theorem 1 is directly applicable.

When the the genus of $\mathcal{C}$ is greater than 1, but the rank of $\mathcal{J}(K)$ is not less than the genus, then Falting's Theorem tells us that $\mathcal{C}(K)$ is still finite, but gives a bound on the number of points which is typically much too large. In such cases, there has has been considerable success with techniques involving covers.

Date: 15 January, 2003.

1991 *Mathematics Subject Classification.* Primary 11G30; Secondary 11G10, 14H40.

Key words and phrases. Coverings of Curves, Descent, Curves of Genus 2, Method of Chabauty.

The first author was supported by EPSRC grant GR/R82975/01. The second author was supported by an EPSRC Research Studentship.

Method 1. *Suppose that $\mathcal{C}$ has at least one known K-rational point P_0 and one wants to find all of $\mathcal{C}(K)$. One first takes an isogeny ϕ, defined over K, from an Abelian variety A to $\mathcal{J}$, the Jacobian of $\mathcal{C}$. For example, we could take $A = \mathcal{J}$, with the isogeny being multiplication by some positive integer m. One tries to compute $\mathcal{J}(K)/\phi(A(K)) = \{D_1, \ldots, D_m\}$ using descent techniques. Let $\mathcal{C}_i$ be the image of $\mathcal{C}$ in $\mathcal{J}$ via $f_i : P \mapsto [P - P_0] - D_i$. Let $\mathcal{D}_i$ be the pullback of $\mathcal{C}_i$ to A via ϕ, and $\mathcal{J}_i$ be the Jacobian of $\mathcal{D}_i$. Every $Q \in \mathcal{C}(K)$ maps to the identity in $\mathcal{J}(K)/\phi(A(K))$ under one of the maps f_i, namely when $D_i = [Q - P_0]$, and so will correspond to a point in $\mathcal{D}_i$. Therefore, to find all of $\mathcal{C}(K)$, it sufficient to find all of $\mathcal{D}_i(K)$ for every i. One can then hope that the rank of $\mathcal{J}_i(K)$ is less than the genus of $\mathcal{D}_i$, for every i, and that Chabauty's Theorem can be applied to find all of $\mathcal{D}_i(K)$.*

There are, of course, many places where this method can potentially fail, but it does at least give a method of attack when Chabauty's Theorem is not directly applicable to the original curve $\mathcal{C}$. One way of trying to find the rank of $\mathcal{J}(K)$, at least in the case where $\mathcal{J}$ is the Jacobian of a hyperelliptic curve $Y^2 = F(X)$ of genus g, and $F(X)$ has odd degree, is to use the injection

$$\begin{array}{rl} q & : \mathcal{J}(K)/2\mathcal{J}(K) \hookrightarrow K[T]/F(T) \cong L_1^*/(L_1^*)^2 \times \ldots \times L_k^*/(L_k^*)^2 \\ & : [\sum_i n_i(X_i, Y_i)] \mapsto [\prod_i (X_i - \alpha_1)^{n_i}, \ldots, \prod_i (X_i - \alpha_k)^{n_i}]. \end{array} \tag{2}$$

Here, we have picked one root α_i of each irreducible factor of $F(X)$, and $L_i = K(\alpha_i)$. If we let $S = \{2, \mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ are the places of bad reduction, then the image of q is contained inside the finite group M, consisting of those $[d_1, \ldots, d_k]$ such that all of the field extensions $L_1(\sqrt{d_1}) : L_1, \ldots, L_k(\sqrt{d_k}) : L_k$ are unramified outside of primes lying over primes of S. Let $\mathfrak{p} \in S$, let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$; then we can use the following commutative diagram

$$\begin{array}{ccc} \mathcal{J}(K)/2\mathcal{J}(K) & \xrightarrow{q} & M \\ \downarrow{\scriptstyle i_\mathfrak{p}} & & \downarrow{\scriptstyle j_\mathfrak{p}} \\ \mathcal{J}(K_\mathfrak{p})/2\mathcal{J}(K_\mathfrak{p}) & \xrightarrow{q_\mathfrak{p}} & M_\mathfrak{p} \end{array} \tag{3}$$

where $q_\mathfrak{p}, M_\mathfrak{p}$ are the local equivalents of q, M, and $i_\mathfrak{p}, j_\mathfrak{p}$ are the maps induced by the natural map $K \hookrightarrow K_\mathfrak{p}$. Then, we can use the fact [5] that

$$\#\mathcal{J}(K_\mathfrak{p})/2\mathcal{J}(K_\mathfrak{p}) = \#\mathcal{J}(K_\mathfrak{p})[2] \cdot (\#\mathfrak{p}/2\mathfrak{p})^g \tag{4}$$

to know when we have found a complete set of generators for $\mathcal{J}(K_\mathfrak{p})/2\mathcal{J}(K_\mathfrak{p})$. The commutativity of (3) gives that $\operatorname{im} q \leqslant j_\mathfrak{p}^{-1}(\operatorname{im} q_\mathfrak{p})$. After intersecting over all $\mathfrak{p} \in S$, we obtain the *2-Selmer bound* on $\#\operatorname{im} q$, which is also a bound on $\#\mathcal{J}(K)/2\mathcal{J}(K)$, since q is an injection. In practice, we cannot guarantee to find the rank of each Jacobian, and typically only an upper bound (such as the above 2-Selmer bound) can be computed, which we hope to be the same as the lower bound obtained from known points.

The literature so far has applied these techniques to a small finite number of naturally occurring examples, and so we do not yet have much of a feeling for the extent to which the techniques can be expected to work generally, or whether there are significant impediments. A natural approach, which we shall adopt here, is to look at infinite families of curves. We shall show that there are infinitely many curves for which a certain covering technique (via bielliptic isogeny) succeeds, and an infinitely family for which it fails. In our

first two families of examples, the Jacobians of the $\mathcal{D}_i$ described in Method 1 split (up to isogeny) into a product of five elliptic curves over $\mathbb{Q}$. Our other family of genus 2 curves is more subtle; the interesting piece of Jacobian of each $\mathcal{D}_i$ is isogenous to the Weil restriction of an elliptic curve over a quadratic number field, which in turn is isogenous to the Jacobian of another related genus 2 curve. We shall show that every member of the family of elliptic curves has nontrivial elements of the Tate-Shafarevich which are killed by a bielliptic isogeny. Furthermore, the new genus 2 curve allows for the potential reapplication of Method 1.

2. Bielliptic Curves of Genus 2

We shall consider curves of genus 2, defined over a number field K

$$\mathcal{C} : Y^2 = F(X) = f_6X^6 + \ldots + f_0, \tag{5}$$

for which there exists an involution $\tau(X) = (aX + b)/(cX + d)$, defined over K, which swaps the roots of $F(X)$; let us say that that τ swaps the six roots of $F(X)$ according to: $\alpha_1 \leftrightarrow \alpha_1'$, $\alpha_2 \leftrightarrow \alpha_2'$, $\alpha_3 \leftrightarrow \alpha_3'$. The matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ associated to τ must have its square equal to $\left(\begin{smallmatrix} k & 0 \\ 0 & k \end{smallmatrix}\right)$ for some $k \in K$, and so has eigenvalues $\pm\sqrt{k}$. There are two involutions of $\mathcal{C}$ given by $(X, Y) \mapsto (\tau(X), \pm k\sqrt{k}Y/(cX + d)^3)$. These two involutions differ by the hyperelliptic involution, and each has two fixed points, namely the two points on $\mathcal{C}$ above the fixed point of τ corresponding to the eigenvalue. By the Riemann-Hurwitz formula, the quotient of $\mathcal{C}$ by each of these involutions is an elliptic curve, and so $\mathcal{C}$ is bielliptic. The above summary can be made more explicit as follows. Let $(s_1\ t_1), (s_2\ t_2)$ be eigenvectors of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ corresponding, respectively, to the eigenvalues $\sqrt{k}$ and $-\sqrt{k}$, so that $(s_1\ t_1)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \sqrt{k}(s_1\ t_1)$ and $(s_2\ t_2)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = -\sqrt{k}(s_2\ t_2)$. When $k \notin (K^*)^2$ we take s_2, t_2 to be the $K(\sqrt{k})$:K conjugates of s_1, t_1, respectively. Then $\sigma(X) = (s_1X + t_1)/(s_2X + t_2)$ is negated by $X \mapsto \tau(X)$, and $\sigma(X)^2$ is invariant. It follows that there exist cubics G^a, G^b defined over $K(\sqrt{k})$ such that $\phi^a : (X, Y) \mapsto (\sigma(X)^2, Y/(s_2X + t_2)^3)$ and $\phi^b : (X, Y) \mapsto (1/\sigma(X)^2, Y/(s_1X + t_1)^3)$ map $\mathcal{C}$ to

$$\mathcal{E}^a : y^2 = G^a(x) = g_3^a x^3 + g_2^a x^2 + g_1^a x + g_0^a, \quad \mathcal{E}^b : \underline{y}^2 = G^b(\underline{x}) = g_3^b \underline{x}^3 + g_2^b \underline{x}^2 + g_1^b \underline{x} + g_0^b, \tag{6}$$

respectively. When $k \notin (K^*)^2$, our choice of σ forces ϕ^b, G^b to be the $K(\sqrt{k})$:K conjugates of ϕ^a, G^a, respectively. When $k \notin (K^*)^2$, let A be Weil restriction of $\mathcal{E}^a$ from $K(\sqrt{k})$ to K; when $k \in (K^*)^2$, let $A = \mathcal{E}^a \times \mathcal{E}^b$. As in [21], these induce the isogeny $\phi = (\phi^a)^* + (\phi^b)^* : A \to \mathcal{J}$, and the dual isogeny $\phi' = (\phi^a)_* \times (\phi^b)_* : \mathcal{J} \to A$. The compositions $\phi' \circ \phi$ and $\phi \circ \phi'$ are the multiplication by 2 maps on A and $\mathcal{J}$, respectively. Let $\mathcal{L}_i$ be the smallest field over which $F_i(X) = (X - \alpha_i)(X - \alpha_i')$ is defined. We shall require the injective homomorphism (a special case of [17]):

$$\begin{aligned} \mu = [\mu_1, \mu_2, \mu_3] \quad &: \mathcal{J}(K)/\phi(A(K)) \hookrightarrow \mathcal{L}_1^*/(\mathcal{L}_1^*)^2 \times \mathcal{L}_2^*/(\mathcal{L}_2^*)^2 \times \mathcal{L}_3^*/(\mathcal{L}_3^*)^2 \\ &: \{(X_1, Y_1), (X_2, Y_2)\} \mapsto [F_1(X_1)F_1(X_2), F_2(X_1)F_2(X_2), F_3(X_1)F_3(X_2)], \end{aligned} \tag{7}$$

where $\{(X_1, Y_1), (X_2, Y_2)\}$ is the common shorthand notation (see p.2 of [5]) used to denote the divisor class $[(X_1, Y_1) + (X_2, Y_2) - \infty^+ - \infty^-]$. For the dual isogeny, there is a similar injective homomorphism

$$\begin{aligned} \mu' = [\mu_1', \mu_2', \mu_3'] \quad &: A(K)/\phi'(\mathcal{J}(K)) \hookrightarrow (\mathcal{L}_1')^*/((\mathcal{L}_1')^*)^2 \times (\mathcal{L}_2')^*/((\mathcal{L}_2')^*)^2 \times (\mathcal{L}_3')^*/((\mathcal{L}_3')^*)^2 \\ &: [(x_1, y_1), (\underline{x}_2, \underline{y}_2)] \mapsto [H_1(x_1, \underline{x}_2), H_2(x_1, \underline{x}_2), H_3(x_1, \underline{x}_2)], \end{aligned} \tag{8}$$

where $H_i(x,\underline{x}) = g_3^a g_3^b (x-\sigma(\alpha_i)^2)(\underline{x}-1/\sigma(\alpha_i)^2)$ and $\mathcal{L}_i'$ is the smallest field over which $H_i(x,\underline{x})$ is defined, for $i=1,2,3$. Suppose that we know at least one $P_0 \in \mathcal{C}(K)$, and that we have computed $\mathcal{J}(K)/\phi(A(K)) = \{D_1,\dots,D_m\}$. Let $\mathcal{C}_i$ be the image of $\mathcal{C}$ in $\mathcal{J}$ via $f_i : P \mapsto [P-P_0]-D_i$. Let $\mathcal{D}_i$ be the pullback of $\mathcal{C}_i$ to A via ϕ, and $\mathcal{J}_i$ be the Jacobian of $\mathcal{D}_i$. From [21] we know that $\mathcal{D}_i$ has genus 5 and that $\mathcal{J}_i$ is isogenous to the Jacobian of $\mathcal{C}$ and the product of the Jacobians of the following three curves of genus 1, defined over $\mathcal{L}_1,\mathcal{L}_2,\mathcal{L}_3$, respectively.

$$\mathcal{E}_{i,j} : y_{i,j}^2 = \mu_j(D_i)F(X)/F_j(X),\ j=1,2,3. \tag{9}$$

In order to find all of $\mathcal{C}(K)$ it is sufficient, for each i, to find all $(X,Y) \in \mathcal{E}_{i,j}(\mathcal{L}_j)$ with $X \in K$, for at least one of $j=1,2,3$. This technique has been used to solve several Diophantine problems ([11],[12],[21]).

Note that, for each of (7) and (8), the third entry is redundant, being the product of the first two entries; this third entry will be suppressed in the computations of the following sections.

3. Coverings of Infinite Families of Curves

If we wish to design an infinite family of examples for which the method fails, the easiest way is to start with a parametrised family of curves such as

$$\mathcal{C}_{\alpha,\beta,\gamma,t} : Y^2 = f_1(X^2)f_2(X^2)f_3(X^2) = (X^2-1+(t-\alpha)^2)(X^2-1+(t-\beta)^2)(X^2-1+(t-\gamma)^2), \tag{10}$$

where $\alpha,\beta,\gamma \in \mathbb{Z}$ are distinct. An examination of the discriminant shows that this is guaranteed to be of genus 2 provided that $t \neq \alpha \pm 1, \beta \pm 1, \gamma \pm 1, (\alpha+\beta)/2, (\beta+\gamma)/2, (\gamma+\alpha)/2$. In the notation of the previous section, take $\tau(X) = -X$, $\sigma(X) = X$ and let ϕ be the bielliptic isogeny from $A = \mathcal{E}^a \times \mathcal{E}^b$ of (6) to the Jacobian $\mathcal{J}$ of $\mathcal{C}_{\alpha,\beta,\gamma,t}$. There will be at least one member of the covering collection $\mathcal{D}_1$ of genus 5 corresponding to the identity element on the Jacobian. The rank of $\mathcal{J}(\mathbb{Q})$ is equal to the sum of the ranks of $\mathcal{E}^a(\mathbb{Q}), \mathcal{E}^b(\mathbb{Q})$. Let us choose $\alpha,\beta,\gamma,t \in \mathbb{Z}$ so that α,β,γ are not in arithmetic progression and no two of them differ by 1. Then, consideration of discriminants shows that the points $(1,(t-\alpha)(t-\beta)(t-\gamma)) \in \mathcal{E}^a(\mathbb{Q})$ and $(0,1) \in \mathcal{E}^b(\mathbb{Q})$ are non-torsion, so that the rank of $\mathcal{J}(\mathbb{Q})$ is at least 2. Furthermore, the Jacobian of $\mathcal{D}_1$ is isogenous to the product of $\mathcal{J}$ and the elliptic curves (9) which, in our case, are isogenous under $(X, y_{1,j}) \mapsto (X^2, Xy_{1,j})$ to the elliptic curves

$$v_{1,1}^2 = xf_2(x)f_3(x),\ v_{1,2}^2 = xf_3(x)f_1(x),\ v_{1,3}^2 = xf_1(x)f_2(x). \tag{11}$$

Our conditions on α,β,γ,t ensure that the points with x-coordinate equal to 1 are all non-torsion. Therefore, the rank of each of these elliptic curves is at least 1 over $\mathbb{Q}$, and the rank of the Jacobian of the genus 5 curve $\mathcal{D}_1$ is at least 5 over $\mathbb{Q}$. This family of examples immediately gives the following negative result.

Lemma 1. *There are infinitely many bielliptic curves $\mathcal{C}$ such that Method 1 fails, when ϕ is taken to be the bielliptic isogeny; that is to say, Chabauty's Theorem does not apply to $\mathcal{C}$, and does not apply to at least one member of the covering collection of curves.*

The above example is rather artificial, in the sense that we made sure that, for any α, β, γ, there was a point defined over the function field $\mathbb{Q}(t)$, forcing the ranks to be at least 1. From now on, our examples will not have such a guaranteed point. We shall include a non-Weierstrass $\mathbb{Q}$-rational base point at infinity, which will typically give a lower bound of 1 on the ranks over $\mathbb{Q}$ of $\mathcal{E}^b$ and the Jacobian of $\mathcal{C}$. We shall consider parametrised families at prime values of the parameter, concentrating on congruence classes where Chabauty's Theorem does not directly apply to $\mathcal{C}$. However, there will be no *a priori* reason in our examples for a lower bound on the ranks over $\mathbb{Q}$ of the 3-dimensional cofactors of each $\mathcal{D}_i$ that remain after the Jacobian of $\mathcal{C}$ has been removed. We shall initially consider genus 2 curves defined over $\mathbb{Q}$, of the form

$$\mathcal{C}_p : Y^2 = (X^2 + 2p)(X^2 + 3p)(X^2 + 4p), \quad \text{where } p \text{ is prime and } p \equiv 5 \text{ or } 7 \pmod 8. \tag{12}$$

In the notation of the previous section, we can take $\sigma(X) = X$, giving the maps $\phi^a : (X, Y) \mapsto (X^2, Y)$ and $\phi^b : (X, Y) \mapsto (1/X^2, Y/X^3)$ to the elliptic curves

$$\mathcal{E}_p^a : y^2 = (x + 2p)(x + 3p)(x + 4p), \;\; \mathcal{E}_p^b : \underline{y}^2 = (2p\underline{x} + 1)(3p\underline{x} + 1)(4p\underline{x} + 1), \tag{13}$$

respectively. We first require the rank of each of these curves.

Lemma 2. *Let $\mathcal{E}_p^a, \mathcal{E}_p^b$ be as in (13), for $p \equiv 5$ or 7 (mod 8). Then $\mathcal{E}_p^a(\mathbb{Q})_{\text{tors}}$ and $\mathcal{E}_p^b(\mathbb{Q})_{\text{tors}}$ each consist only of the identity and three points of order 2. The rank of $\mathcal{E}_p^b(\mathbb{Q})$ is 1, with $(0, 1)$ being a generator for $\mathcal{E}_p^b(\mathbb{Q})$ modulo torsion. The rank of $\mathcal{E}_p^a(\mathbb{Q})$ is also 1 and there is a generator (x, y) of $\mathcal{E}_p^a(\mathbb{Q})$ modulo torsion, satisfying $[x + 2p, x + 3p] = [-1, -1]$ modulo squares (when $p \equiv 5$ (mod 8)) and $[2, 1]$ modulo squares (when $p \equiv 7$ (mod 8)).*

Proof First note that, for any p, the map $(x, y) \mapsto (px, y)$ is a birational equivalence between $\mathcal{E}_p^b$ and the curve $\underline{y}^2 = (2z + 1)(3z + 1)(4z + 1)$. Reductions modulo 5 and 7 show that $\mathcal{E}_p^b(\mathbb{Q})_{\text{tors}}$ consists only of the identity and three points of order 2, and a standard complete 2-descent and height argument on the curve shows it to have rank 1 with generator $(0, 1)$ of $\mathcal{E}_p^b(\mathbb{Q})$ modulo torsion.

The curves $\mathcal{E}_p^a$ genuinely depend on p. Reduction modulo 3 shows that $\mathcal{E}_p^a(\mathbb{Q})_{\text{tors}}$ consists only of the identity and three points of order 2. Further, $\mathcal{E}_p^a$ is birationally equivalent over $\mathbb{Q}$ to the curve $y^2 = s^3 - p^2 s$, which is a special case of the elliptic curve related to the congruent number problem, and is well known to have rank proved unconditionally to be 1, since any prime congruent to 5 or 7 modulo 8 is known unconditionally to be a congruent number (see [1],[16],[19]).

Let $p \equiv 5 \pmod 8$. In Diagram (3), we can take our map $q : \mathcal{E}_p^a(\mathbb{Q})/2\mathcal{E}_p^a(\mathbb{Q}) \hookrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (x, y) \mapsto [x+2p, x+3p]$, with the redundant third entry $x+4p$ omitted, since it is the product $(x+2p)(x+3p)$. We can also take $M = \langle [-1, 1], [2, 1], [p, 1], [1, -1], [1, 2], [1, p] \rangle$. Now, $\ker j_\infty = \langle [2, 1], [p, 1], [1, 2], [1, p] \rangle$ and $q_\infty : (-3p, 0) \mapsto [-p, -1]$, and so, in view of (4), $\mathcal{E}_p^a(\mathbb{R})/2\mathcal{E}_p^a(\mathbb{R}) = \langle (-3p, 0) \rangle$. Similarly, since -1, but not 2, is a quadratic residue mod p, we have $\ker j_p = \langle [-1, 1], [1, -1] \rangle$ and $q_p : (-2p, 0), (-3p, 0) \mapsto [2, p], [-p, -1]$, which are independent in ${\mathbb{Q}_p}^*/({\mathbb{Q}_p}^*)^2 \times {\mathbb{Q}_p}^*/({\mathbb{Q}_p}^*)^2$. In view of (4), $\mathcal{E}_p^a(\mathbb{Q}_p)/2\mathcal{E}_p^a(\mathbb{Q}_p) = \langle (-2p, 0), (-3p, 0) \rangle$. Finally, $\ker j_2$ is trivial, and $q_2 : (-2p, 0), (-3p, 0), (p/4, \epsilon) \mapsto [2, p], [-p, -1], [p, 1]$, which are independent in

${\mathbb{Q}_2}^*/({\mathbb{Q}_2}^*)^2 \times {\mathbb{Q}_2}^*/({\mathbb{Q}_2}^*)^2$; here $\epsilon \in \mathbb{Q}_2$ is such that $\epsilon^2 = (p/4+2p)(p/4+3p)(p/4+4p) = 1989p^3/64$, which exists since $1989p^3 \equiv 1 \pmod 8$. In view of (4), $\mathcal{E}_p^a(\mathbb{Q}_2)/2\mathcal{E}_p^a(\mathbb{Q}_2) = \langle(-2p,0),(-3p,0),(p/4,\epsilon)\rangle$. We can now compute the 2-Selmer group as the intersection of $j_{\mathfrak{p}}^{-1}(q_{\mathfrak{p}}(\mathcal{E}_p^a(\mathbb{Q}_{\mathfrak{p}})/2\mathcal{E}_p^a(\mathbb{Q}_{\mathfrak{p}})))$ over $\mathfrak{p} = \infty, p, 2$. From the above computations, we see that this is:

$$\langle \ker j_\infty, [-p,-1]\rangle \cap \langle \ker j_p, [2,p],[-p,-1]\rangle \cap \langle \ker j_2, [2,p],[-p,-1],[p,1]\rangle = \langle [2,p],[-p,-1],[-1,-1]\rangle. \quad (14)$$

The first two generators are images under q of the known 2-torsion points. Since the rank is 1, there must be a generator of $\mathcal{E}_p^a(\mathbb{Q})$ modulo torsion, which maps to $[-1,-1]$ under q.

An almost identical argument shows that, for $p \equiv 7 \pmod 8$, a generator of $\mathcal{E}_p^a(\mathbb{Q})$ modulo torsion maps to $[2,1]$ under q. □

Since the Jacobian $\mathcal{J}_p$ of $\mathcal{C}_p$ is isogenous to $\mathcal{E}_p^a \times \mathcal{E}_p^b$, the following is immediate.

Corollary 1. *Let $\mathcal{C}_p$ be as in (12) with Jacobian $\mathcal{J}_p$, for $p \equiv 5,7$ (mod 8). Then the rank of $\mathcal{J}_p(\mathbb{Q})$ is 2.*

In the other cases $p \equiv 1,3 \pmod 8$, it is straightforward to show that sign of the functional equation corresponding to $\mathcal{E}_p^a$ is always $+1$, and so conjecturally $\mathcal{E}_p^a(\mathbb{Q})$ should have average rank 0 or close to 0 (see [4],[13]). We are not interested in these cases, since typically the rank of $\mathcal{J}_p(\mathbb{Q})$ is 1 and the rank of $\mathcal{E}_p^a(\mathbb{Q})$ is 0, so that it will typically be trivial to show that $\mathcal{C}_p(\mathbb{Q}) = \{\infty^+, \infty^-\}$.

Returning to the cases we are considering, namely $p \equiv 5,7 \pmod 8$, we have seen that the rank of $\mathcal{J}_p(\mathbb{Q})$ is 2, and so we cannot apply Chabauty's technique to find all of $\mathcal{C}_p(\mathbb{Q})$. In this respect, there is no distinction between the cases $p \equiv 5 \pmod 8$ and $p \equiv 7 \pmod 8$. However, as we shall see in a moment, there is a difference between the behaviours of these cases under pullbacks via the bielliptic isogeny.

Lemma 3. *Let $\mathcal{J}_p$ be the Jacobian of the curve $\mathcal{C}_p$ in (12). If $p \equiv 5$ (mod 8) then $\mathcal{J}_p(\mathbb{Q})/\phi(A(\mathbb{Q}))$ consists only of the identity. If $p \equiv 7$ (mod 8) then $\mathcal{J}_p(\mathbb{Q})/\phi(A(\mathbb{Q}))$ has order 2, consisting of the identity and a non-identity element mapped to $[2,1]$ by μ of (7).*

Proof Since ϕ, ϕ' are 4-isogenies, the sum of the 2-ranks of $\mathcal{J}_p(\mathbb{Q})/\phi(A(\mathbb{Q}))$ and $A(\mathbb{Q})/\phi'(\mathcal{J}_p(\mathbb{Q}))$ has to be 4 more than the rank of $\mathcal{J}_p(\mathbb{Q})$. The elements $[(-2p,0),\infty], [(-3p,0),\infty], [\infty,(-1/2p,0)], [\infty,(-1/3p,0)]$, $[\infty,(0,1)]$ map to $[2,p],[-p,-1],[6,-1],[1,-2],[3,2]$ under the map μ' of (8). These are all independent members of $\mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$. We know from Lemma 2 and Corollary 1 that $\mathcal{J}_p(\mathbb{Q})$ has rank 2 and $\mathcal{E}^a(\mathbb{Q})$ has rank 1 with infinite generator P, where $[P,\infty]$ maps to $[-1,-1]$ or $[2,1]$ when $p \equiv 5,7 \pmod 8$, respectively. For the case $p \equiv 5 \pmod 8$, this is independent of the above 5 members of $\mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$, and so $\mathcal{J}_p(\mathbb{Q})/\phi(A(\mathbb{Q}))$ is trivial. For the case $p \equiv 7 \pmod 8$, we are missing a generator; a standard local analysis of the maps μ, μ' of (7),(8) shows that this must correspond to a nontrivial $D \in \mathcal{J}_p(\mathbb{Q})/\phi(A(\mathbb{Q}))$ which is mapped to $[2,1]$ by μ. □

We first dispose of the case $p \equiv 5 \pmod 8$.

Theorem 2. *Let $\mathcal{C}_p$ be as in (12), with $p \equiv 5$ (mod 8). Then $\mathcal{C}_p(\mathbb{Q}) = \{\infty^+, \infty^-\}$.*

Proof In view of Lemma 3, it is only necessary to find the $\mathbb{Q}$-rational points on any one of the curves $\mathcal{E}_{1,j}$ as in (9), where F_1, F_2, F_3 are the three quadratic factors in (12). As in the previous example, we can use $(X, y_{1,j}) \mapsto (X^2, Xy_{1,j})$ to the elliptic curves

$$\mathcal{E}_{1,1} : v_{1,1}^2 = x(x+3p)(x+4p),\ \mathcal{E}_{1,2} : v_{1,2}^2 = x(x+4p)(x+2p),\ \mathcal{E}_{1,3} : v_{1,3}^2 = x(x+2p)(x+3p). \tag{15}$$

We can now imitate the proof of Lemma 2 to show that, when $p \equiv 5 \pmod{24}$, the 2-Selmer bounds on the ranks are 1,0,0, respectively; when $p \equiv 13 \pmod{24}$, the 2-Selmer bounds on the ranks are 0,0,1, respectively. In all cases, there is no $\mathbb{Q}$-rational torsion outside 2-torsion. One sees that there is always a rank 0 curve available (indeed, the second curve can always be used) which gives $x = 0, -3p, -4p$ as the only available x-coordinates of affine points, none of which have preimages in $\mathcal{C}_p(\mathbb{Q})$. □

Note that this is a nontrivial application of Method 1, since Chabauty is not directly applicable to the original curve $\mathcal{C}_p$ which has genus 2 and rank of $\mathcal{J}_p(\mathbb{Q})$ equal to 2. The single covering curve has genus 5, with Jacobian of rank at most 3.

Corollary 2. *There are infinitely many curves for which Method 1 successfully finds all of $\mathcal{C}(\mathbb{Q})$.*

When $p \equiv 7 \pmod 8$, there are two covering curves $\mathcal{D}_1, \mathcal{D}_2$, and we shall see that Method 1 is defied by $\mathcal{D}_1$ when $p \equiv 23 \pmod{24}$.

Theorem 3. *Let $\mathcal{C}_p$ be as in (12), with $p \equiv 7$ (mod 8). The pullbacks $\mathcal{D}_i$, $i = 1, 2$, associated to the two members of $\mathcal{J}_p(\mathbb{Q})/\phi(A(\mathbb{Q}))$ have Jacobians isogenous to the product of $\mathcal{J}_p$ and elliptic curves $\mathcal{E}_{i,j}$, $j = 1, 2, 3$, where the 2-Selmer bounds on the ranks over $\mathbb{Q}$ of $\mathcal{E}_{1,j}$, $j = 1, 2, 3$, are $0, 1, 0$ or $1, 1, 1$ (for $p \equiv 7$ or 23 mod 24, respectively) and the 2-Selmer bounds on the ranks over $\mathbb{Q}$ of $\mathcal{E}_{2,j}$, $j = 1, 2, 3$, are $2, 1, 1$ or $1, 1, 2$ (for $p \equiv 7$ or 23 mod 24, respectively), which are too large for Method 1 to be applied.*

Proof To resolve $\mathcal{D}_1$, it is only necessary to find the $\mathbb{Q}$-rational points on any one of the curves $\mathcal{E}_{1,j}$ as in (9), where F_1, F_2, F_3 are the three quadratic factors in (12). As in the previous example, we can use $(X, y_{1,j}) \mapsto (X^2, Xy_{1,j})$ to the elliptic curves

$$\mathcal{E}_{1,1} : v_{1,1}^2 = x(x+3p)(x+4p),\ \mathcal{E}_{1,2} : v_{1,2}^2 = x(x+4p)(x+2p),\ \mathcal{E}_{1,3} : v_{1,3}^2 = x(x+2p)(x+3p). \tag{16}$$

We can now imitate the proof of Lemma 2 to show that these curves have 2-Selmer bounds on the ranks over $\mathbb{Q}$ given by $0, 1, 0$, respectively, when $p \equiv 7 \pmod{24}$, and have no $\mathbb{Q}$-rational torsion outside 2-torsion. Similarly, they have 2-Selmer bounds on the rank over $\mathbb{Q}$ given by $1, 1, 1$, respectively, when $p \equiv 7 \pmod{24}$, and have no $\mathbb{Q}$-rational torsion outside 2-torsion.

For $\mathcal{D}_2$, the corresponding elliptic curves are

$$\mathcal{E}_{2,1} : v_{2,1}^2 = 2x(x+3p)(x+4p),\ \mathcal{E}_{2,2} : v_{2,2}^2 = x(x+4p)(x+2p),\ \mathcal{E}_{2,3} : v_{2,3}^2 = 2x(x+2p)(x+3p). \tag{17}$$

An imitation of the proof of Lemma 2 shows that the 2-Selmer bounds on the ranks are as stated. □

The elliptic curves $\mathcal{E}_{1,2}, \mathcal{E}_{2,2}$ are both birationally equivalent over $\mathbb{Q}$ to $y^2 = s^3 - (2p)^2 s$, which is known to have rank 1 over $\mathbb{Q}$ unconditionally, since twice any prime congruent to 7 modulo 8 is unconditionally

a congruent number (see [1],[16],[19]). For $p \equiv 23 \pmod{24}$, the standard conjecture that the 2-Selmer bound and actual rank have the same parity, gives that all three elliptic curves $\mathcal{E}_{1,j}$ have rank 1, and so the Jacobian of $\mathcal{D}_1$ has rank 5. This then gives another infinite family of curves for which Method 1 fails, as in Lemma 1. Indeed, this is a less contrived example than that of Lemma 1, since we have not artificially created a known $\mathbb{Q}$-rational point of infinite order on the elliptic curves (16). For the instances of 2-Selmer bound 2, both rank 0 and rank 2 are attained for particular values of p; for example, $\mathcal{E}_{2,1}(\mathbb{Q})$ has rank 2 and 0 when $p = 7, 31$, respectively, and $\mathcal{E}_{2,3}(\mathbb{Q})$ has rank 0 and 2 when $p = 23, 47$, respectively.

More subtle examples can be obtained when the elliptic curves associated to the covers are not defined over $\mathbb{Q}$. Consider the family of curves of genus 2

$$\mathfrak{C}_p : Y^2 = (X^2+p)(X^4+p^2) = (X^2+p)(X^2-pi)(X^2+pi), \quad \text{where } p \text{ is prime and } p \equiv 7 \pmod{8}. \tag{18}$$

In the notation of the previous section, we can again take $\sigma(X) = X$, giving the maps $\phi^a : (X,Y) \mapsto (X^2, Y)$ and $\phi^b : (X,Y) \mapsto (1/X^2, Y/X^3)$ to the elliptic curves

$$\mathfrak{E}_p^a : y^2 = (x+p)(x^2+p^2), \quad \mathfrak{E}_p^b : \underline{y}^2 = (p\underline{x}+1)(p^2\underline{x}^2+1), \tag{19}$$

as usual inducing an isogeny $\phi : A \to \mathfrak{J}_p$, where $A = \mathfrak{E}_p^a \times \mathfrak{E}_p^b$ and $\mathfrak{J}_p$ is the Jacobian of $\mathfrak{C}_p$. The map μ of (7) becomes, in this case,

(20)
$$\begin{aligned} \mu = [\mu_1, \mu_2, \mu_3] \quad &: \mathfrak{J}(\mathbb{Q})/\phi(A(\mathbb{Q})) \hookrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}(i)^*/(\mathbb{Q}(i)^*)^2 \times \mathbb{Q}(i)^*/(\mathbb{Q}(i)^*)^2 \\ &: \{(X_1,Y_1),(X_2,Y_2)\} \mapsto [(X_1^2+p)(X_2^2+p), ((X_1^2-pi)(X_2^2-pi), (X_1^2+pi)(X_2^2+pi)]. \end{aligned}$$

For any p, the map $(x,y) \mapsto (px, y)$ is a birational equivalence between $\mathfrak{E}_p^b$ and the curve $\underline{y}^2 = (z+1)(z^2+1)$; it is straightforward to check directly that this has rank 1 over $\mathbb{Q}$, with infinite generator $(0,1)$, and that the torsion group over $\mathbb{Q}$ consists only of the identity and a point of order 2. The curves $\mathfrak{E}_p^a$ genuinely depend on p, and have fortunately been analysed in [20], where the rank over $\mathbb{Q}$ is shown to be bounded above by $3, 0, 0, 1$, when $p \equiv 1, 3, 5, 7 \pmod{8}$, respectively, on performing a descent via isogeny (and the torsion group over $\mathbb{Q}$ is shown to consist only of the identity and a point $(-p, 0)$ of order 2). We are not considering the cases $p \equiv 3, 5 \pmod{8}$, since the rank of $\mathcal{J}_p(\mathbb{Q})$ is 1 and the rank of $\mathfrak{E}_p^a(\mathbb{Q})$ is 0, so that it will typically be trivial to show that $\mathfrak{C}_p(\mathbb{Q}) = \{\infty^+, \infty^-\}$. We are also not considering the complicated case $p \equiv 1 \pmod{8}$, where rank 1 and 3 both occur for $\mathfrak{E}_p^a(\mathbb{Q})$. Returning to the case we are considering, namely $p \equiv 7 \pmod{8}$, it is shown in [20] that the Selmer bound on the rank of $\mathfrak{E}_p^a(\mathbb{Q})$ is 1. Therefore, the rank is exactly 1, subject to standard parity conjectures. Indeed, the sign of the functional equation is shown to be -1 in [20], so that rank $= 1$ also follows from the conjectures of Birch and Swinnerton-Dyer. It is also pointed out in [20] that it should be possible to prove unconditionally that the rank is exactly 1 using Heegner points on a modular curve, as explained in [1]. An actual generator is found for all $p \equiv 7 \pmod{8}$ and $p < 300$ in [20]. Overall, then, we can be confident that each of the curves $\mathfrak{E}_p^a, \mathfrak{E}_p^b$ has rank 1 over $\mathbb{Q}$, and that $\mathfrak{J}_p$ has rank 2 over $\mathbb{Q}$. Using similar arguments to Lemma 3 gives the following.

Lemma 4. *Let $\mathfrak{C}_p$ be as in (18), with Jacobian $\mathfrak{J}_p$, and let $A = \mathfrak{E}_p^a \times \mathfrak{E}_p^b$, where $\mathfrak{E}_p^a, \mathfrak{E}_p^b$ are as in (19), with the natural bielliptic isogeny $\phi : A \to \mathfrak{J}_p$. Then $\mathfrak{J}_p(\mathbb{Q})$ has rank 1 or 2. In the first case, $\mathfrak{J}_p(\mathbb{Q})/\phi(A(\mathbb{Q}))$*

consists only of the identity. in the second case, $\mathfrak{J}_p(\mathbb{Q})/\phi(A(\mathbb{Q})) = \{D_1, D_2\}$*, where* D_1 *is the identity and* D_2 *maps to* $[2, 1+i, 1-i]$ *under the map* μ *in (20).*

In view of Lemma 4, we can try to resolve $\mathcal{D}_1$ by considering the curves $\mathcal{E}_{1,j}$ as in (9), where F_1, F_2, F_3 are the three quadratic factors in (18). As before, we can use $(X, y_{1,j}) \mapsto (X^2, Xy_{1,j})$ to the elliptic curves

$$\mathcal{E}_{1,1} : v_{1,1}^2 = x(x^2+p^2),\ \mathcal{E}_{1,2} : v_{1,2}^2 = x(x+p)(x+pi),\ \mathcal{E}_{1,3} : v_{1,3}^2 = x(x+p)(x-pi). \tag{21}$$

The first of these, $\mathcal{E}_{1,1}$, is an elliptic curve over $\mathbb{Q}$, and standard techniques bound the rank above by 1. Indeed this is 2-isogenous over $\mathbb{Q}$ to $y^2 = s^3 - (2p)^2 s$ which, as we have already commented (immediately after the proof of Theorem 3), is known to have rank 1 over $\mathbb{Q}$ unconditionally. Therefore, this curve is of no use in resolving $\mathcal{D}_1$. It is also sufficient to find all points over $\mathbb{Q}(i)$ on the second curve, $\mathcal{E}_{1,2}$, with $x \in \mathbb{Q}$. We can attempt to apply elliptic curve Chabauty techniques, as in [2],[3],[10], provided that the rank over $\mathbb{Q}(i)$ is at most 1. The second and third curves are conjugates, and so only one of them need be considered.

Lemma 5. *Let* $\mathcal{E}_{1,2}$ *be the elliptic curve* $v_{1,2}^2 = x(x+p)(x+pi)$*, defined over* $\mathbb{Q}(i)$*, where* p *is a prime and* $p \equiv 7$ *(mod 8). Then* $\mathcal{E}_{1,2}(\mathbb{Q}(i))_{\text{tors}}$ *consists only of the identity and three points of order* 2*, and the* 2*-Selmer bound on the rank over* $\mathbb{Q}(i)$ *of* $\mathcal{E}_{1,2}$ *is 2.*

Proof Reduction modulo 3 to $\widetilde{\mathcal{E}}_{1,2}(\mathbb{F}_3(i))$ gives the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$; but none of the points of order 2 in $\mathcal{E}_{1,2}(\mathbb{Q}(i))_{\text{tors}}$ is in $2\mathcal{E}_{1,2}(\mathbb{Q}(i))$. This shows that $\mathcal{E}_{1,2}(\mathbb{Q}(i))_{\text{tors}}$ consists only of the identity and three points of order 2.

In Diagram (3), our map $q : \mathcal{E}_{1,2}(\mathbb{Q}(i))/2\mathcal{E}_{1,2}(\mathbb{Q}(i)) \hookrightarrow \mathbb{Q}(i)^*/(\mathbb{Q}(i)^*)^2 \times \mathbb{Q}(i)^*/(\mathbb{Q}(i)^*)^2 : (x,y) \mapsto [x, x+p]$ can have the redundant third entry $x+pi$ omitted, since it is the product $x(x+p)$. We can also take $M = \langle [i,1], [1+i,1], [p,1], [1,i], [1,1+i], [1,p] \rangle$. No information can be obtained at infinity, since $\mathbb{C}^*/(\mathbb{C}^*)^2$ is the trivial group. Since 2, but not -1, is a quadratic residue mod p, we have $\ker j_p = \langle [i,1], [1+i,1], [1,i], [1,1+i] \rangle$ and $q_p : (0,0), (-p,0) \mapsto [i,p], [p, i(1+i)]$, which are independent in $\mathbb{Q}(i)_p^*/(\mathbb{Q}(i)_p^*)^2 \times \mathbb{Q}(i)_p^*/(\mathbb{Q}(i)_p^*)^2$. In view of (4), $\mathcal{E}_p^a(\mathbb{Q}(i)_p)/2\mathcal{E}_p^a(\mathbb{Q}(i)_p) = \langle (0,0), (-p,0) \rangle$. Finally, we localise at $\mathbb{Q}(i)_{1+i}$; here $\ker j_{1+i} = \langle [p,1], [1,p] \rangle$, and $q_{1+i} : (0,0), (-p,0), (4i, \epsilon_1), (3+\frac{i}{2}, \epsilon_2) \mapsto [i,p], [p, i(1+i)], [i,3], [1+2i, 3]$, which are independent in $\mathbb{Q}(i)_{1+i}^*/(\mathbb{Q}(i)_{1+i}^*)^2 \times \mathbb{Q}(i)_{1+i}^*/(\mathbb{Q}(i)_{1+i}^*)^2$; here $\epsilon_1, \epsilon_2 \in \mathbb{Q}(i)_{1+i}$ are such that $\epsilon_1^2 = 4i(4i+p)(4i+pi), \epsilon_2^2 = (3+\frac{i}{2})(3+\frac{i}{2}+p)(3+\frac{i}{2}+pi)$. In view of (4), $\mathcal{E}_{1,2}(\mathbb{Q}(i)_{1+i})/2\mathcal{E}_{1,2}(\mathbb{Q}(i)_{1+i}) = \langle (0,0), (-p,0), (4i,\epsilon_1), (3+\frac{i}{2}, \epsilon_2) \rangle$. Note that none of $\langle [i,3], [1+2i,3] \rangle$, apart from the identity $[1,1]$, have preimages under j_{1+i}. We can now compute the 2-Selmer group as the intersection of $j_{\mathfrak{p}}^{-1}(q_{\mathfrak{p}}(\mathcal{E}_{1,2}(\mathbb{Q}(i)_{\mathfrak{p}})/2\mathcal{E}_{1,2}(\mathbb{Q}(i)_{\mathfrak{p}})))$ over $\mathfrak{p} = \infty, p, 1+i$. From the above computations, we see that this is:

$$\langle \ker j_p, [i,p], [p, i(1+i)] \rangle \cap \langle \ker j_{1+i}, [i,p], [p,i(1+i)] \rangle = \langle [p,1], [1,p], [i,p], [p, i(1+i)] \rangle. \tag{22}$$

The last two generators are images under q of the known 2-torsion points. It follows that the 2-Selmer bound on the rank is 2 and that, if the rank is 2 then there are generators of $\mathcal{E}_{1,2}(\mathbb{Q}(i))$ modulo torsion, which map to $[p,1], [1,p]$ under q. □

After experimentation, one suspects that this is not the best bound that can be attained. This is due to members of the Tate-Shafarevich group, as will become apparent in the next section.

For $\mathcal{D}_2$, the corresponding elliptic curves are

$$\mathcal{E}_{2,1} : v_{2,1}^2 = 2x(x^2+p^2),\ \mathcal{E}_{2,2} : v_{2,2}^2 = (1+i)x(x+p)(x+pi),\ \mathcal{E}_{2,3} : v_{2,3}^2 = (1-i)x(x+p)(x-pi). \tag{23}$$

The first of these is 2-isogenous over $\mathbb{Q}$ to $y^2 = s^3 - p^2 s$, which is known to have rank 1 over $\mathbb{Q}$ unconditionally, since any prime congruent to 7 modulo 8 is known unconditionally to be a congruent number (see [1],[16],[19]). The second and third curves are conjugate and so, as before, only one of them needs to be considered. The situation here is as for Lemma 5.

Lemma 6. *Let $\mathcal{E}_{2,2}$ be the elliptic curve $v_{2,2}^2 = (1+i)x(x+p)(x+pi)$, defined over $\mathbb{Q}(i)$, where p is a prime and $p \equiv 7$ (mod 8). Then $\mathcal{E}_{2,2}(\mathbb{Q}(i))_{\rm tors}$ consists only of the identity and three points of order 2, and the 2-Selmer bound on the rank over $\mathbb{Q}(i)$ of $\mathcal{E}_{2,2}$ is 2.*

Proof Everything is as for the proof of Lemma 5, except that $(3+i, \epsilon_1')$, $(\frac{7}{2}+\frac{5}{2}i, \epsilon_2')$ are the two new generators of $\mathcal{E}_{2,2}(\mathbb{Q}(i)_{1+i})/2\mathcal{E}_{2,2}(\mathbb{Q}(i)_{1+i})$; these are mapped by q_{1+i} to $[i(1+2i), 3i(1+i)(1+2i)], [3(1+2i), 3i]$, respectively, Again, none of $\langle [i(1+2i), 3i(1+i)(1+2i)], [3(1+2i), 3i]\rangle$, apart from the identity $[1,1]$, have preimages under j_{1+i}, and so the same argument as in Lemma 5 gives that the 2-Selmer bound on the rank is 2 and that, if the rank is 2 then there are generators of $\mathcal{E}_{2,2}(\mathbb{Q}(i))$ modulo torsion, which map to $[p,1], [1,p]$ under q. □

4. Members of the Tate-Shafarevich Group killed by the bielliptic Isogeny

The elliptic curves defined over $\mathbb{Q}(i)$ in (21),(23), are of the form $v^2 = q(x)\ell(x)$, where $q(x)$ is defined over $\mathbb{Q}$ and $\ell(x)$ is defined over the quadratic field $\mathbb{Q}(i)$. We are trying to find all points defined over $\mathbb{Q}(i)$ on these curves with $x \in \mathbb{Q}$. Letting $v = r + si$, we get two equations in x, r, s; we can eliminate r, and get a single polynomial equation in x, s, in which s only occurs to even powers. This is a genus 0 equation in x, t, where $t = s^2/q(x)$. If this genus 0 equation has no $\mathbb{Q}$-rational points, then there are no points on our original elliptic curve with $x \in \mathbb{Q}$, and we are finished. Otherwise, we can find a parametrisation $x(z), t(z)$ of the genus 0 curve. Then $s^2 = t(z)q(x(z))$ gives a curve of genus 2, defined over $\mathbb{Q}$, and it is sufficient to find all $\mathbb{Q}$-rational points on this curve. Furthermore, the map $(z,s) \mapsto (x,v)$ induces a $\mathbb{Q}$-rational isogeny from the Jacobian of this genus 2 curve to the Weil restriction from $\mathbb{Q}(i)$ to $\mathbb{Q}$ of the original elliptic curve.

Applying this process to the second elliptic curve in (21), we let $v_{1,2} = r + si$, and equate the coefficients of 1 and i to get the two equations

$$2rs = px^2 + p^2 x, \quad r^2 - s^2 = x^3 + px^2. \tag{24}$$

Solving the first equation for r and substituting into the second equation gives an equation in x, s which can be written

$$4tx = -4t^2 + p^2, \tag{25}$$

where $t = s^2/(x^2+px)$. The general solution to this genus 0 equation can be parametrised by $x(z) = (-4z^2+p^2)/4z$ and $t(z) = z$. Then $s^2 = t(z)(x(z)^2+px(z))$ gives the genus 2 curve

$$s^2 = (4z^2-p^2)(4z^2-p^2-4pz)/16z, \tag{26}$$

so that

$$\mathcal{C}_{1,2} : Y^2 = X(X+2p)(X+4p)(X^2-8p^2), \tag{27}$$

where $X = 4z-2p, Y = 32sz$. Combining these transformations gives the following map from $\mathcal{C}_{1,2}$ to $\mathcal{E}_{1,2}$.

$$(X,Y) \mapsto \big(-X(X+4p)/4(X+2p), Y(iX+2ip+2p)/8(X+2p)^2\big). \tag{28}$$

For the second elliptic curve in (23), we let $v_{2,2} = r+si$ and, proceeding as above, we get

$$x^2 = 4t^2+4xt-2px-4pt-p^2, \tag{29}$$

where $t = s^2/(x^2+px)$. We can use $x = -p, t = 0$ as a base point to give the parametrisation $x(z) = -p(4z^2-4z-1)/(4z^2+4z-1)$ and $t(z) = 8pz^2/(4z^2+4z-1)$. Then $s^2 = t(z)(x(z)^2+px(z))$ gives the genus 2 curve

$$s^2 = -64p^3z^3(4z^2-4z-1)/(4z^2+4z-1)^3, \tag{30}$$

so that

$$\mathcal{C}_{2,2} : Y^2 = X^5-24p^2X^3+16p^4X = X(X^2+4pX-4p^2)(X^2-4pX-4p^2), \tag{31}$$

where $X = -p/z, Y = 8ps(4z^2+4z-1)^2/z^4$. Combining these transformations gives the following map from $\mathcal{C}_{2,2}$ to $\mathcal{E}_{2,2}$.

$$(X,Y) \mapsto \big(-p(X^2-4pX-4p^2)/(X^2+4pX-4p^2), 4Y(X-2ip)p^2/(X^2+4pX-4p^2)^2\big). \tag{32}$$

In summary, we have the following connection between $\mathcal{C}_{1,2}, \mathcal{C}_{2,2}$ and $\mathcal{E}_{1,2}, \mathcal{E}_{2,2}$.

Lemma 7. *Let $\mathcal{E}_{1,2}, \mathcal{E}_{2,2}$ be as in Lemmas 5,6, and let $\mathcal{C}_{1,2}, \mathcal{C}_{2,2}$ be as in (27),(31), with Jacobians $J_{1,2}, J_{2,2}$, respectively. Then $J_{1,2}, J_{2,2}$ are isogenous over $\mathbb{Q}$ to the Weil restrictions from $\mathbb{Q}(i)$ to $\mathbb{Q}$ of $\mathcal{E}_{1,2}, \mathcal{E}_{2,2}$, respectively, and so the ranks of $J_{1,2}(\mathbb{Q}), J_{2,2}(\mathbb{Q})$ are the same as the ranks of $\mathcal{E}_{1,2}(\mathbb{Q}(i)), \mathcal{E}_{2,2}(\mathbb{Q}(i))$, respectively.*

Note that we now have a description, up to isogeny, of the Jacobians of two genus 5 curves $\mathcal{D}_1, \mathcal{D}_2$ which cover the genus 2 curve $\mathfrak{C}_p$ of (18). The Jacobian of $\mathcal{D}_1$ is isogenous to the product of: the Jacobian of $\mathfrak{C}_p$, the elliptic curve $\mathcal{E}_{1,1}$ in (21), and the Jacobian of the genus 2 curve $\mathcal{C}_{1,2}$ in (27). Since the first two of these factors have ranks 2 and 1 over $\mathbb{Q}$, it is $\mathcal{C}_{1,2}$ which is the important piece of $\mathcal{D}_1$. Similarly, the Jacobian of $\mathcal{D}_2$ is isogenous to the product of: the Jacobian of $\mathfrak{C}_p$, the elliptic curve $\mathcal{E}_{2,1}$ in (23), and the Jacobian of the genus 2 curve $\mathcal{C}_{2,2}$ in (31). Again, the first two of these factors have ranks 2 and 1 over $\mathbb{Q}$, and it is $\mathcal{C}_{2,2}$ which is the important piece. In order to compute $\mathfrak{C}_p(\mathbb{Q})$ it is sufficient to compute $\mathcal{C}_{1,2}(\mathbb{Q})$ and $\mathcal{C}_{2,2}(\mathbb{Q})$. The ranks of $J_{1,2}(\mathbb{Q}), J_{2,2}(\mathbb{Q})$ are the same as the ranks of $\mathcal{E}_{1,2}(\mathbb{Q}(i)), \mathcal{E}_{2,2}(\mathbb{Q}(i))$, for which we have already computed the 2-Selmer bounds in the last section. However, as we shall see, there is a potential benefit in attempting a complete 2-descent directly on $J_{1,2}(\mathbb{Q}), J_{2,2}(\mathbb{Q})$, since there may be an

improvement in the 2-Selmer bounds. It turns out that the Selmer group computations are different for the subclasses $p \equiv 7 \pmod{16}$ and $p \equiv 15 \pmod{16}$. The difference is partly a consequence of the following technical lemma about quadratic residues, whose proof was provided for us independently by Noam Elkies and Hendrik Lenstra.

Lemma 8. *Let $p \equiv 7$ (mod 8) be prime, and let $\gamma \in \mathbb{F}_p$ be such that $\gamma^2 = 2$ in $\mathbb{F}_p$. When $p \equiv 7$ (mod 16), we have $\gamma \in (\mathbb{F}_p^*)^2 \iff 1+\gamma \notin (\mathbb{F}_p^*)^2$. When $p \equiv 15$ (mod 16), we have $\gamma \in (\mathbb{F}_p^*)^2 \iff 1+\gamma \in (\mathbb{F}_p^*)^2$.*

Proof Let z be a primitive 16th root of unity, and let $x = z^2 + 1/z^2, y = z + 1/z$ so that $\mathbb{F}_p \subseteq \mathbb{F}_p(x) \subseteq \mathbb{F}_p(y) \subseteq \mathbb{F}_p(z)$, with each extension being of degree at most 2. Then $x^2 = z^4 + 2 + 1/z^4 = 2$, so that $\gamma = x$ or $-x$. Let $p \equiv 7 \pmod{16}$. Then: $(x+2)^{(p-1)/2} = (y^2)^{(p-1)/2} = y^{p-1} = (y^p)/y = ((z+1/z)^p)/y = (z^p + 1/z^p)/y = (z^7 + 1/z^7)/y = z^8(1/z + z)/y = -1$, so that $x + 2 \notin (\mathbb{F}_p^*)^2$. Similarly, $-x + 2 \notin (\mathbb{F}_p^*)^2$. Whether $\gamma = x$ or $-x$ we have $\gamma(1+\gamma) = \gamma + 2 \notin (\mathbb{F}_p^*)^2$, so that $\gamma \in (\mathbb{F}_p^*)^2 \iff 1+\gamma \notin (\mathbb{F}_p^*)^2$, as required.

Let $p \equiv 15 \pmod{16}$. Then: $(x+2)^{(p-1)/2} = (y^2)^{(p-1)/2} = y^{p-1} = (y^p)/y = ((z+1/z)^p)/y = (z^p + 1/z^p)/y = (z^{15} + 1/z^{15})/y = (1/z + z)/y = 1$, so that $x + 2 \in (\mathbb{F}_p^*)^2$. Similarly, $-x + 2 \in (\mathbb{F}_p^*)^2$. Whether $\gamma = x$ or $-x$ we have $\gamma(1+\gamma) = \gamma + 2 \in (\mathbb{F}_p^*)^2$, so that $\gamma \in (\mathbb{F}_p^*)^2 \iff 1+\gamma \in (\mathbb{F}_p^*)^2$, as required. □

Since $(2^{(p+1)/4})^2 = 2$ in $\mathbb{F}_p$, for any $p \equiv 7 \pmod{8}$, we can express the above result as an evaluation of a Legendre symbol.

Corollary 3. *Let $p \equiv 7$ (mod 8) be prime. Then $\left(\frac{2^{(p+1)/4}+1}{p}\right) = (-1)^{(p+1)/8}$.*

Another reason for the difference between the subclasses is the following lemma.

Lemma 9. *Let $p \equiv 7$ (mod 8) be prime; then there exist positive $a, b \in \mathbb{Z}$ such that $a^2 - 2b^2 = p$. For any such a, b, the group $\langle -1, 1+\sqrt{2}, a+b\sqrt{2}\rangle$ is of order 8 or 4 in $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$ when $p \equiv 7$ or 15 (mod 16), respectively.*

Proof The existence of a, b is an immediate consequence of the fact that 2 is a quadratic residue mod p, and unique factorisation in $\mathbb{Z}[\sqrt{2}]$. For $p \equiv 7 \pmod{16}$, it is a finite computation to check that any such a, b satisfy $a \equiv 3, 5 \pmod 8$ and $b \equiv 1, 3, 5, 7 \pmod 8$; it is then a further finite computation to check that none of $-1, \pm(1+\sqrt{2}), \pm(a+b\sqrt{2}), \pm(1+\sqrt{2})(a+b\sqrt{2})$ are squares in $\mathbb{Z}[\sqrt{2}]$ modulo 8, and so $-1, 1+\sqrt{2}, a+b\sqrt{2}$ are independent in $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$, as required. For $p \equiv 15 \pmod{16}$, it is a finite computation to check that any such a, b satisfy $a \equiv 1, 7 \pmod 8$ and $b \equiv 1, 3, 5, 7 \pmod 8$; it is then a further finite computation to check that none of $-1, \pm(1+\sqrt{2})$ are squares in $\mathbb{Z}[\sqrt{2}]$ modulo 8, but that exactly one of $\pm(1+\sqrt{2})(a+b\sqrt{2})$ is a square in $\mathbb{Z}[\sqrt{2}]$ modulo 8 and so, by Hensel's Lemma, is in $(\mathbb{Q}_2(\sqrt{2})^*)^2$. □

We are now in a position to compute the 2-Selmer groups of our two Jacobians.

Lemma 10. *Let $\mathcal{C}_{1,2}, \mathcal{C}_{2,2}$ be as in (27),(31), with Jacobians $J_{1,2}, J_{2,2}$, respectively. The 2-Selmer bound on the rank of $J_{1,2}(\mathbb{Q})$ is 0 when $p \equiv 7$ (mod 16), and is 2 when $p \equiv 15$ (mod 16). The 2-Selmer bound on the rank of $J_{2,2}(\mathbb{Q})$ is 2 for all $p \equiv 7$ (mod 8). In all cases, there is no torsion over $\mathbb{Q}$ outside 2-torsion.*

Proof We shall present the details only for the curve $\mathcal{C}_{1,2}$, for the case $p \equiv 7 \pmod{16}$, the proof of the other cases being similar. The 2-torsion subgroup of $J_{1,2}(\mathbb{Q})$ is of order 8, generated by

$$\mathfrak{A}_1 = [(0,0) - \infty],\ \mathfrak{A}_2 = [(-2p,0) - \infty],\ \mathfrak{A}_3 = [(-4p,0) - \infty]. \tag{33}$$

The only finite primes dividing the discriminant are $2, p$. A finite computation shows that $\#\widetilde{J}_p(\mathbb{F}_3) = 8$, and so $J_{1,2}(\mathbb{Q})_{\text{tors}} \mid 8$. Since we already know eight members of $J_{1,2}(\mathbb{Q})_{\text{tors}}$, these must give all of $J_{1,2}(\mathbb{Q})_{\text{tors}}$.

To show that $J_{1,2}(\mathbb{Q})$ has rank zero it is sufficient to show that $\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3$ generate $J_{1,2}(\mathbb{Q})/2J_{1,2}(\mathbb{Q})$. We can take the injective map of (2) to be

$$\begin{aligned} q &: J_{1,2}(\mathbb{Q})/2J_{1,2}(\mathbb{Q}) \hookrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}(\sqrt{2})^*/\left(\mathbb{Q}(\sqrt{2})^*\right)^2, \\ &: \left[\sum (X_i, Y_i)\right] \mapsto \left[\prod (X_i + 2p), \prod (X_i + 4p), \prod (X_i - 2p\sqrt{2})\right]. \end{aligned} \tag{34}$$

Note that the other two linear components can be suppressed since $\prod(X_i + 2p\sqrt{2})$ is the $\mathbb{Q}(\sqrt{2})$:$\mathbb{Q}$ conjugate of $\prod(X_i - 2p\sqrt{2})$, and $\prod X_i = \prod(X_i + 2p)(X_i + 4p)(X_i - 2p\sqrt{2})(X_i + 2p\sqrt{2})$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

Since $2, p$ are the only finite primes of bad reduction,

$$\begin{aligned} \text{im } q \leq \quad M = \quad & \langle [-1,1,1], [2,1,1], [p,1,1], [1,-1,1], [1,2,1], [1,p,1], \\ & [1,1,-1], [1,1,1+\sqrt{2}], [1,1,\sqrt{2}], [1,1,a+b\sqrt{2}], [1,1,a-b\sqrt{2}] \rangle, \end{aligned}$$

where $a, b \in \mathbb{Z}^+$ are such that $a^2 - 2b^2 = p$, which must exists since $p \equiv 7 \pmod 8$. Now we can see that the members of $J_p(\mathbb{Q})$ given in (33) map as follows,

$$\mathfrak{A}_1 \mapsto [2p, p, -p\sqrt{2}],\ \mathfrak{A}_2 \mapsto [1, 2p, -p(1+\sqrt{2})],\ \mathfrak{A}_3 \mapsto [-2p, 1, -p(1+\sqrt{2})\sqrt{2}], \tag{35}$$

so that $H \leq \text{im } q$, where

$$H = \langle [2p, p, -p\sqrt{2}], [1, 2p, -p(1+\sqrt{2})], [-2p, 1, -p(1+\sqrt{2})\sqrt{2}] \rangle. \tag{36}$$

At $\mathfrak{p} = \infty$ we have in (3),

$$\ker j_\infty = \langle [2,1,1], [p,1,1], [1,2,1], [1,p,1], [1,1,\sqrt{2}(1+\sqrt{2})], [1,1,a+b\sqrt{2}], [1,1,a-b\sqrt{2}] \rangle, \tag{37}$$

so that $\mathfrak{A}_2, \mathfrak{A}_3$ are independent members of $J_{1,2}(\mathbb{R})/2J_{1,2}(\mathbb{R})$. We know $\#J_{1,2}(\mathbb{R})/2J_{1,2}(\mathbb{R}) = 2^2$ from (4), so that $J_{1,2}(\mathbb{R})/2J_{1,2}(\mathbb{R}) = \langle \mathfrak{A}_2, \mathfrak{A}_3 \rangle$. The commutativity of Diagram (3) tells us that

$$\text{im } q \leq \langle [1, 2p, -p(1+\sqrt{2})], [-2p, 1, -p(1+\sqrt{2})\sqrt{2}], \ker j_\infty \rangle. \tag{38}$$

Now consider $\mathfrak{p} = p$. Since $p \equiv 7 \pmod 8$, we have $2 \in (\mathbb{Q}_p^*)^2$, but $-1, -2 \notin (\mathbb{Q}_p^*)^2$. Since $p \equiv 7 \pmod{16}$, Lemma 8 implies that $-2 - \sqrt{2} \in (\mathbb{Q}_p^*)^2$, for either choice of $\sqrt{2} \in \mathbb{Q}_p$. In (3) we now have

$$\ker j_p = \langle [2,1,1], [1,2,1], [1,1,-2-\sqrt{2}] \rangle, \tag{39}$$

so that $\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3, \mathfrak{A}_4$ are independent members of $J_{1,2}(\mathbb{Q}_p)/2J_{1,2}(\mathbb{Q}_p)$, where $\mathfrak{A}_4 = [(2p\gamma, 0) - \infty]$ and γ is chosen so that $\gamma^2 = 2$ and $\gamma \in (\mathbb{Q}_p^*)^2$ (the facts that $2 \in (\mathbb{Q}_p^*)^2$ and $-1 \notin (\mathbb{Q}_p^*)^2$ guarantee the existence of such a γ). Note that $j_p([-p, -p, \delta]) = q_p(\mathfrak{A}_4)$, where δ is one of the four possibilities $\pm(a \pm b\sqrt{2})$; it makes no difference to the structure of the following computations which of these four possibilities occurs,

so without loss of generality say that $\delta = -(a - b\sqrt{2})$. We know $\#J_{1,2}(\mathbb{Q}_p)/2J_{1,2}(\mathbb{Q}_p) = 2^4$ from (4), so that $J_{1,2}(\mathbb{Q}_p)/2J_{1,2}(\mathbb{Q}_p) = \langle \mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3, \mathfrak{A}_4 \rangle$. The commutativity of Diagram (3) tells us that

$$\text{im } q \leq \langle [2p, p, -p\sqrt{2}], [1, 2p, -p(1+\sqrt{2})], [-2p, 1, -p(1+\sqrt{2})\sqrt{2}], [-p, -p, -(a-b\sqrt{2})], \ker j_p \rangle. \tag{40}$$

Finally let us consider $\mathfrak{p} = 2$. Since $p \equiv 7 \pmod 8$ we have $-p \in (\mathbb{Q}_2^*)^2$ and indeed a finite computation, together with Lemma 9, shows that in (3),

$$\ker j_2 = \langle [-p, 1, 1], [1, -p, 1], [1, 1, -p] \rangle, \tag{41}$$

so that $\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3$ are independent members of $J_{1,2}(\mathbb{Q}_2)/2J_{1,2}(\mathbb{Q}_2)$. We know $\#J_{1,2}(\mathbb{Q}_2)/2J_{1,2}(\mathbb{Q}_2) = 2^5$ from (4), and so we are still missing two generators. Let $\mathfrak{A}_5 = [(6, \epsilon_1) - \infty], \mathfrak{A}_6 = [(7, \epsilon_2) - \infty] \in J_{1,2}(\mathbb{Q}_2)$, where $\epsilon_1, \epsilon_2 \in \mathbb{Q}_2$ satisfy $\epsilon_1^2 = 6(6+2p)(6+4p)(6^2 - 8p^2)$ and $\epsilon_2^2 = 7(7+2p)(7+4p)(7^2 - 8p^2)$. Then $\mathfrak{A}_5 \mapsto [-3, 2, 3+\sqrt{2}]$ and $\mathfrak{A}_6 \mapsto [-3, 3, -1+2\sqrt{2}]$ under q_2. These images are independent from each other and from the images of $\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3$, and so $\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3, \mathfrak{A}_5, \mathfrak{A}_6$ generate $J_{1,2}(\mathbb{Q}_2)/2J_{1,2}(\mathbb{Q}_2)$. No member of M maps to 3 under j_2, and so $\mathfrak{A}_5, \mathfrak{A}_6$ do not contribute any new preimages under j_2. Hence we have from commutativity of Diagram 3

$$\text{im } q \leq \langle [2p, p, -p\sqrt{2}], [1, 2p, -p(1+\sqrt{2})], [-2p, 1, -p(1+\sqrt{2})\sqrt{2}], \ker j_2 \rangle. \tag{42}$$

Intersecting the three groups in (38),(40),(42) gives H, so that im $q = H$ and the rank of $J_{1,2}(\mathbb{Q})/2J_{1,2}(\mathbb{Q}) = 0$, as required. □

The difference between the Selmer rank bounds in Lemmas 5,10 immediately proves the existence of members of the Tate-Shafarevich group killed by the bielliptic isogeny, for every curve in an infinite family.

Theorem 4. *Let $\mathcal{E}_{1,2} : v_{1,2}^2 = x(x+p)(x+pi)$, as in Lemma 5. Then there are nontrivial members of the 2-part of the Tate-Shafarevich group when $p \equiv 7$ (mod 16).*

Proof The map (28) induces a $\mathbb{Q}$-rational isogeny from $J_{1,2}$ to the Weil restriction from $\mathbb{Q}(i)$ to $\mathbb{Q}$ of $\mathcal{E}_{1,2}$, so that the rank of $J_{1,2}(\mathbb{Q})$ is the same as the rank of $\mathcal{E}_{1,2}(\mathbb{Q}(i))$. The complete 2-descent in Lemma 5 gave a 2-Selmer bound of 2 on the rank of $\mathcal{E}_{1,2}(\mathbb{Q}(i))$. Lemma 10 showed the rank of $J_{1,2}(\mathbb{Q})$, and hence the rank of $\mathcal{E}_{1,2}(\mathbb{Q}(i))$ to be 0, giving the required member of the 2-part of the Tate-Shafarevich group. □

Recall that, at the end of the proof of Lemma 5, it was shown that $\mathcal{E}_{1,2}(\mathbb{Q}(i))$ modulo torsion is mapped by q to $\langle [p, 1], [1, p] \rangle$, and so we can use the formula in [18], p.281, to write explicit models for the three homogeneous spaces, defined over $\mathbb{Q}(i)$,

$$\begin{array}{lcl} \mathcal{H}[p,1] & : & p(z_1^2+1) = z_2^2, \quad z_1^2 + i = z_3^2, \\ \mathcal{H}[1,p] & : & z_1^2 + p = pz_2^2, \quad z_1^2 + pi = pz_3^2, \\ \mathcal{H}[p,p] & : & z_1^2 + 1 = z_2^2, \quad p(z_1^2+i) = z_3^2. \end{array} \tag{43}$$

The three left hand equations are conics in z_1, z_2, which can be parametrised using the base points $(i, 0)$, $(0, 1)$, $(0, 1)$, respectively, and the parametrisation of z_1 can be substituted into each right hand equation to get a plane curve. We can then obtain the birational transformations

$$\begin{array}{lll} (z_1, z_2, z_3) & \mapsto (z, w) = (z_2(z_1+i)/(z_1^2+1), z_3(z_2^2 - pz_1^2 + 2piz_1 + p)/(z_1 - i)^2), \\ (z_1, z_2, z_3) & \mapsto (z, w) = ((z_2 - 1)/z_1, z_3(-z_1^2 + pz_2^2 - 2pz_2 + p)/z_1^2), \\ (z_1, z_2, z_3) & \mapsto (z, w) = ((z_2 - 1)/z_1, z_3(z_2 + z_1 - 1)(z_2 - z_1 - 1)/z_1^2), \end{array} \tag{44}$$

from the three curves in (43) to the following three plane curve models of the homogeneous spaces:

$$\begin{array}{lcl} \mathcal{H}'[p,1] & : & w^2 = (i-1)(z^4+2piz^2+p^2), \\ \mathcal{H}'[1,p] & : & w^2 = i(p^2z^4-2pz^2-4piz^2+1), \\ \mathcal{H}'[p,p] & : & w^2 = pi(z^4-2z^2-4iz^2+1). \end{array} \tag{45}$$

In view of Lemmas 5,10, each of these three curves, defined over $\mathbb{Q}(i)$, must violate the Hasse principle when $p \equiv 7 \pmod{16}$.

As well as determining the rank for a subcongruence class of primes, obtaining the equations for $\mathcal{C}_{1,2}$ and $\mathcal{C}_{2,2}$ also has the benefit that we are now set up, if we desire, to perform a repeated application of the process. For example, the x-coordinates of the Weierstrass points on $\mathcal{C}_{1,2}$ are permuted by the involution $X \mapsto -2p(X+4p)/(X+2p)$. The F_i of (7) are then $F_1(X) = X+2p$, $F_2(X) = X(X+4p)$, $F_3(X) = X^2-8p^2$, and we already have for free the isogeny $\phi_{1,2}$ from the $\mathbb{Q}(i)$:$\mathbb{Q}$ Weil restriction of $\mathcal{E}_{1,2}$ to $J_{1,2}$, namely the isogeny induced by the map (28). If we now perform a repeated application of the method described in Section 2, pulling back along ϕ, the Jacobians of our covers will include pieces isogenous to the Jacobians of, for example, twists of the genus 1 curves $y_1^2 = x(x+4p)(x^2-8p^2)$ and $y_2^2 = (x+2p)(x^2-8p^2)$. Taking $v = \frac{1}{4}(x^2-8p^2)/(x+2p)$, which is invariant under the involution, we see that $v(v^2+2pv+2p^2)$ and $(v+p)(v^2+2pv+2p^2)$ are both squares, giving rise to elliptic curves in Weierstrass form isogenous to the Jacobians of these genus 1 curves. The common quadratic in v allows us to deduce that $v(v+p)$ is a square, and so (repeating our usual trick) the parametrisation $v(t) = p/(t^2-1)$ can be substituted into the first cubic to give a new genus 2 curve: $s^2 = v(t)(v(t)^2+2pv(t)+2p^2)$, which will be one of the covering curves in the second application of the method.

Note that the method is 'up-down' with respect to each involution τ. We move 'up' from two elliptic curves $\mathcal{E}^a, \mathcal{E}^b$, as in (6), to the genus 2 curve $\mathcal{C} : Y^2 = F(X)$ such that the X-coordinate maps from $\mathcal{C}$ to $\mathcal{E}^a, \mathcal{E}^b$ are invariant under the involution. Our covering process gives rise to genus 1 curves $y_1^2 = Q_1(X), y_2^2 = Q_2(X)$, using (9); we then obtain quadratic maps invariant under the same involution τ, which take us back 'down' to elliptic curves in Weierstrass form, as in (11),(15),(16),(17). In our example, we have performed this process first with the involution $X \mapsto -X$ and then with the involution $X \mapsto -2p(X+4p)/(X+2p)$. The resulting genus 2 curves will continue to be bielliptic; there seems to be no explosion in the discriminants of the new curves, and we suppose (although have not proved) that the sequence of curves of genus 2 over $\mathbb{Q}$ obtained in this way, have only $2, p$ as finite primes of bad reduction. This would mean that there are only finitely many available, and the process would eventually repeat. This has methodological implications, since it is possible to imagine curves which are entirely resistant to repeated applications. In such cases, there are still many other options for trying to determine $\mathcal{C}(\mathbb{Q})$, such as pulling back along the entire multiplication by 2 map.

When covering techniques are applied, as here, to obtain a collection of curves $\mathcal{D}_i$ whose rational points cover those of our starting curve $\mathcal{C}$, the portions which determine the success or failure of the method are the cofactors of the Jacobians of the $\mathcal{D}_i$, once the Jacobian of $\mathcal{C}$ has been removed, and whether Chabauty techniques can be applied to these cofactors. These techniques are primarily required when Chabauty's

Theorem fails to be applicable to the original curve $\mathcal{C}$. A heuristic analysis of the likelihood of success of covering methods will be a difficult task; however, one aspect of such an analysis will be the question of whether larger than average rank of the Jacobian of $\mathcal{C}$ will lead to larger than average rank of these cofactors. When there are points on $\mathcal{C}(\mathbb{Q})$ apart from the point P_0 (and its hyperelliptic involute) required as a base point to derive the covers, then there will surely be some such bias, as each such rational point will induce nonzero rank on one of the cofactors, as was certainly the case in (10), where the points with $X = 1$ on (10) induced non-torsion points with $x = 1$ on the elliptic curves (11) occurring in the cofactor. However, our subsequent families of examples (12),(18) were constructed without a bias of this type (note that ∞^+, ∞^- in all of our examples (10),(12),(18) map to torsion on (11),(15),(16),(17),(21),(23) and do not contribute to the ranks). For the genus 2 curve given in (12), with $p \equiv 5, 7 \pmod 8$, we have a bias in the Jacobian of our starting curve towards high rank, since it is the product of two elliptic curves over $\mathbb{Q}$, each of rank 1, which is higher than the 'expected' average of 1/2, or at least very close to 1/2 (see [4],[13]), as opposed to the cases we have ignored, namely $p \equiv 1, 3 \pmod 8$, where we expect $\mathcal{E}_p^a(\mathbb{Q})$ to have average rank 0, or at least very close to 0. Interestingly, this bias in our choice of starting curve (12) does create a mild bias towards large rank of the elliptic curves involved in the 3-dimensional cofactors of the Jacobians of $\mathcal{D}_1, \mathcal{D}_2$. Using Theorems 2,3, and giving equal weight to each of $p \equiv 5, 7, 13, 23 \pmod{24}$, we see that there are 18 elliptic curves occurring, with a Selmer bound of 0 (and so rank 0) occurring 6 times, a Selmer bound of 1 (and so conjecturally rank 1) occurring 10 times, and a Selmer bound of 2 (with both ranks 0 and 2 occurring for particular values of p, but with expected average rank 0, or at least very close to 0) occurring 2 times. The 18 elliptic curves involved in the cofactors therefore conjecturally have, on average, a rank total of 10, and so the average rank per curve is 1/18 more than the conjectured 'average' rank of 1/2 (or at least very close to 1/2) over all elliptic curves, in the sense explained in [4]. We observe that the amount that this rank total of 10 is above what one would expect of a 'random' collection of 18 elliptic curves is $1 = 10 - 9$, which is the same amount that our starting elliptic curves $\mathcal{E}_p^a, \mathcal{E}_p^b$ in (13) have rank sum larger than expected, namely $1 = 2 - 1$.

References

[1] B.J. Birch. Heegner points of elliptic curves. *Symp. Math. Inst. Alta Math.* , **15** (1975), 441–445.

[2] N. Bruin. Chabauty methods using covers on curves of genus 2. http://www.math.leidenuniv.nl/reports/1999-15.shtml

[3] N. Bruin. KASH-based program for performing 2-descent on elliptic curves over number fields. Available from: http://www.math.uu.nl/people/bruin/ell.shar

[4] A. Brumer. The average rank of elliptic curves. I. Invent. Math., **109** (1992), 445–472.

[5] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* LMS–LNS **230**. Cambridge University Press, Cambridge, 1996.

[6] C. Chabauty. Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension. *C. R. Acad. Sci. Paris*, **212** (1941), 1022–1024.

[7] R.F. Coleman. Effective Chabauty, *Duke Math. J.*, **52** (1985), 765–780.

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

[9] 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.

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

[11] E.V. Flynn. On Q-derived polynomials. *Proc. Edinburgh Math. Soc.* **44** (2001), 103–110.

[12] E.V. Flynn and J.L. Wetherell. Covering collections and a challenge problem of Serre. *Acta Arith.* **XCVIII.2** (2001), 197–205.
[13] N.M. Katz. *Twisted L-Functions and Monodromy.* AM-**150**, Princeton University Press, Princeton, 2002.
[14] W.G. McCallum. The arithmetic of Fermat curves. *Math. Ann.* **294** (1992), 503–511.
[15] W.G. McCallum. On the method of Coleman and Chabauty. *Math. Ann.* **299** (1994), no. 3, 565–596.
[16] P. Monsky. Mock Heegner points and congruent numbers. *Math. Z.* **204** (1990), no. 1, 45–67.
[17] E.F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.*, **310** (1998), no. 3, 447–471.
[18] J.H. Silverman. *The Arithmetic of Elliptic Curves.* GTM **106**. Springer-Verlag, 1986.
[19] N.M. Stephens. Congruence properties of congruent numbers. Bull. London Math. Soc. **7** (1975), 182–184.
[20] R.J. Stroeker and J. Top. On the equation $Y^2 = (X + p)(X^2 + p^2)$. *Rocky Mountain Journal of Mathematics*, **24** (1994), no. 3, 1135–1161.
[21] J.L. Wetherell. Bounding the number of rational points on certain curves of high rank. PhD Dissertation, University of California at Berkeley, 1997.

Mathematical Institute, University of Oxford, 24–29 St. Giles, Oxford OX1 3LB, England
E-mail address: flynn@maths.ox.ac.uk

Department Mathematical Sciences, University of Liverpool, Liverpool L69 3BX, England
E-mail address: J.Redmond@liverpool.ac.uk