Chabauty methods using covers on curves of genus 2

Nils Bruin

August 16, 1999

Abstract

In this article, we consider the problem of determining the set of rational points on curves of genus 2. Given a curve $\mathcal{C}$ of genus 2 over a number field, we demonstrate a finite set of degree 16 unramified covers such that the rational points of $\mathcal{C}$ are covered by the rational points of the covers. We show that these covers map to elliptic curves, making Chabauty methods practically feasible on them. This gives a possibility to determine the rational points on genus 2 curves with Jacobians of higher rank. As an example, we determine the primitive rational solutions to the equation $x^2 + y^3 = z^8$, which involves finding the rational points on some genus 2 curves with Jacobians of rank 2.

1 Introduction

In 1941 (see [Cha41]), Chabauty proved Mordell's conjecture (Faltings' theorem) in the special situation where the Mordell–Weil rank of the Jacobian is less than the genus of the curve. His method is still important since, unlike Faltings' proof, it gives a construction that often yields a sharp bound on the number of rational points on the curve. This paper demonstrates a way of using Chabauty's construction indirectly if the Mordell–Weil rank is at least the genus.

The method of unramified covers, as applied in this paper, was first employed successfully by Wetherell (see [Wet97]) to bielliptic curves of genus 2. The construction given here is essentially a generalisation of his method. We do take a slightly different point of view, though, and by using the methods explained in [Bru99b], we avoid doing any arithmetic on objects of dimension > 1 directly.

Consider a curve $\mathcal{C}$ of genus 2 over $\mathbb{Q}$. Given a rational point on $\mathcal{C}$, we can embed $\mathcal{C}$ in $\mathcal{J} := \mathrm{Jac}_{\mathcal{C}}$. Since $\mathcal{J}$ is an abelian variety, it comes equipped with several endomorphisms. One of them is the multiplication-by-2 map $[2] : \mathcal{J} \to \mathcal{J}$. It is of degree 16 and, since it is a group homomorphism, it is unramified. If we pull $\mathcal{C}$ back along $[2]$, then we get a degree 16 unramified cover $[2] : \mathcal{D} \to \mathcal{C}$. Naturally, $[2](\mathcal{D}(\mathbb{Q})) \subset \mathcal{C}(\mathbb{Q})$, but in general, equality need not hold. As we will show, there is a finite set of twists $[2]_\delta : \mathcal{D}_\delta \to \mathcal{C}$ of the cover $[2]$, classified by $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$, such that $\bigcup_\delta [2]_\delta(\mathcal{D}_\delta(\mathbb{Q})) = \mathcal{C}(\mathbb{Q})$. As it turns out, the map $[2]$ combined with the hyperelliptic cover $\mathcal{C} \to \mathbb{P}_1$ factors through 15 elliptic curves $\mathcal{E}_{\delta,T}$, classified by the 15 non-trivial 2-torsion points of $\mathcal{J}$. It follows that, geometrically, the Jacobian of the genus 17 curve $\mathcal{D}$ is isogenous to the product of $\mathcal{J}$ and those 15 elliptic curves. Let $L := \mathbb{Q}(T)$ be the field of definition of the 2-torsion point T. Then $\mathcal{E}_{\delta,T}$ is defined over L as well.

$$\begin{tikzcd}
 & \mathcal{D}_\delta \arrow[r, hook] \arrow[dl, "\pi"'] \arrow[dr] & \mathcal{J} \arrow[dr, "{[2]}"] & \\
E_{\delta,T} \arrow[dr, "\varphi"'] & & \mathcal{C} \arrow[r, hook] \arrow[dl, "\cdot/\langle\hat{\cdot}\rangle"] & \mathcal{J} \\
 & \mathbb{P}_1 & &
\end{tikzcd}$$

As the diagram above suggests, a way of finding $\mathcal{D}_\delta(\mathbb{Q})$ is to determine those points of $\mathcal{E}_{\delta,T}(L)$ that have an image in $\mathbb{P}_1(\mathbb{Q})$ under φ. This set might well be finite. Consequently, it is straightforward to check which points lift to rational points on $\mathcal{D}_\delta$. Alternatively, we can just look at the (finite) set $\varphi(\mathcal{E}_{\delta,T}(L)) \cap \mathbb{P}_1(\mathbb{Q})$ and see which values lift to rational points on $\mathcal{C}$. If we do this for all relevant values of δ representing classes of $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ then we have determined $\mathcal{C}(\mathbb{Q})$. Provided that $\mathrm{rk}(\mathcal{E}_{\delta,T}(L)) < [L : \mathbb{Q}]$, a way of determining $\varphi(\mathcal{E}_{\delta,T}(L)) \cap \mathbb{P}_1(\mathbb{Q})$ is discussed in [Bru99b].

The rank conditions on the elliptic curves are independent from $\mathrm{rk}(\mathcal{J}(\mathbb{Q}))$ and therefore this method provides a possibility of determining the rational points even for high $\mathrm{rk}(\mathcal{J}(\mathbb{Q}))$, where normal Chabauty methods as described in [FPS97], [Fly97], [CF96] and [Bru97] require $\mathrm{rk}(\mathcal{J}(\mathbb{Q}))$ to be low.

Note that if $[L : \mathbb{Q}] = 15$, i.e. if all 2-torsion is conjugate, then the elliptic curves would have to be of rank at least 15 to form an obstruction. It might lead to practical problems to apply the method in [Bru99b] for such high degree fields, though. If the 2-torsion points lie in different conjugacy classes, then if $\mathcal{E}_{\delta,T}$ violates the rank criterion for one T, we can try a T in a different conjugacy class.

Note that a high $\mathrm{rk}(\mathcal{J}(\mathbb{Q}))$ leads to a large $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ and therefore potentially leads to a large number of $\mathcal{D}_\delta$ to be considered. For each of those δ, we have to find a $T \in \mathcal{J}[2]$ such that $\mathcal{E}_{\delta,T}$ satisfies the rank criterion. Therefore, this method is still somewhat sensitive to $\mathrm{rk}(\mathcal{J}(\mathbb{Q}))$ and it is not yet clear if this will ever lead to problems in practise.

As an example of the feasibility of this method, we prove the following theorem.

Theorem 1.1 *The only integer, pairwise prime, solutions to $x^8 + y^3 = z^2$ are*

$$(x, y, z) \in \{(\pm 1, 0, \pm 1), (0, 1, \pm 1), (\pm 1, 2, \pm 3), (\pm 43, 96222, \pm 30042907)\}.$$

This supplements earlier results in [Bru97] and [Bru99b]. These articles, together with the present one, form material from [Bru99a]. Analogously to [Bru97], we prove the theorem above by determining the rational points on several curves of genus 2. Two of those curves turn out to have Jacobians of Mordell–Weil rank 2. These have 2-torsion points over degree

3 and 12 extensions of $\mathbb{Q}$. Some of the elliptic curves related to the degree 3 points turn out to violate the rank criterion. Therefore, we apply the described method to elliptic curves over degree 12 extensions over $\mathbb{Q}$. They turn out to be of Mordell–Weil rank 4. It should be noted that the elliptic curves have a 2-torsion point over their field of definition, which means that the ranks could be determined using a 2-isogeny descent (see [Bru99b]).

2 Multiplication-by-two cover on genus 2

In this section we construct a covering collection of unramified covers of a curve $\mathcal{C}$ of genus 2 such that each rational point of $\mathcal{C}$ is covered by a rational point on one of the covers. For this, we use the multiplication by 2 map on the Jacobian of $\mathcal{C}$. Furthermore, we show that, apart from $\mathcal{C}$, these new curves cover elliptic curves, possibly over an extension of the base field. This enables us to translate the question of determining the rational points on the covers into finding points on elliptic curves satisfying some rationality conditions. A method for finding such points is explained in [Bru99b].

Let K be a number field (in our applications, $K = \mathbb{Q}$) and let $\mathcal{C}$ be a curve over K of genus 2, given by a model

$$\mathcal{C} : Y^2 = F(X) = f_6(X - t_1)(X - t_2) \cdots (X - t_6)$$

where $F \in \mathcal{O}_K[X]$ is a square-free polynomial of degree 5 or 6. If $\deg(F) = 5$ then we write $t_i = \infty$ for one i. The map $(X, Y) \mapsto (X, -Y)$ defines an involution on $\mathcal{C}$ and is denoted by $P \mapsto \hat{P}$. The fixed points of this involution are exactly the $T_i = (t_i, 0)$. If $\deg(F) = 5$, then we have that one of the $T_i = \infty$. Otherwise, $\mathcal{C}$ has two points corresponding to the singular point ∞ of the model, denoted by ∞^+ and ∞^-. These can be distinguished by the value of Y/X^3.

Let $\mathcal{J}$ denote the jacobian variety of $\mathcal{C}$. We fix some notation for some morphisms $\mathcal{J} \to \mathcal{J}$ as a variety. Since $\mathcal{J}$ is an abelian variety, we have that $\mathbb{Z}$ acts on $\mathcal{J}$ by multiplication. We denote this with $[n] : \mathcal{J} \to \mathcal{J}$. Any $D_0 \in \mathcal{J}(\bar{K})$ can be identified with the translation $D \mapsto D + D_0$.

We refer to [CF96] for an explanation of the arithmetic on $\mathcal{J}$. We just recall that points of $\mathcal{J}(\bar{K})$ can be represented by formal finite linear combinations $\sum_{P \in \mathcal{C}(\bar{K})} n_P P$ with $n_P \in \mathbb{Z}$ and $\sum n_P = 0$. We have that $[-1](\sum n_P P) = \sum n_P \hat{P}$. We see that the points $T_{ij} = [T_i - T_j]$ are 2-torsion points. One further relation is that $T_{12} + T_{34} + T_{56} = 0$. As a consequence, $\mathcal{J}[2](\bar{K})$ consists of 16 elements and the 15 non-zero elements give involutions $T_{ij} : \mathcal{J} \to \mathcal{J}$ given by $D \mapsto D + T_{ij}$.

Suppose we have $P_0 \in \mathcal{C}(K)$. Then we can embed $\mathcal{C}(K)$ in $\mathcal{J}(K)$ using the Abel-Jacobi map $P \mapsto [P - P_0]$. The image of this map constitutes the curve $\mathcal{C}_{P_0} \subset \mathcal{J}$. Note that the hyperelliptic involution on $\mathcal{C}_{P_0}$ is induced by $[\hat{P}_0 - P_0] \circ [-1]$.

Define $\mathcal{D}_{P_0}$ to be the inverse image of $\mathcal{C}_{P_0}$ under the [2]-map. Thus, $\mathcal{D}_{P_0}$ is an unramified degree 16 cover of a genus 2 curve which, by Riemann–Hurwitz, is of genus 17. Note that $\mathcal{D}_{P_0}(K)$ need not cover the whole of $\mathcal{C}_{P_0}(K)$, since fibres of rational points might consist of conjugate points. However, $\mathcal{D}_{P_0}(K)$ certainly does cover P_0. For another point $P_1 \in \mathcal{C}(K)$, we have that $\mathcal{C}_{P_1}$ is isomorphic to $\mathcal{C}_{P_0}$ over K by the translation $[P_0 - P_1]$. Similarly, $\mathcal{D}_{P_1}$ is isomorphic to $\mathcal{D}_{P_0}$ over $\bar{K}$ via the translation over some point D such that $2D = [P_0 - P_1]$. Thus, we see that $\mathcal{D}_{P_1}$ is a twist of $\mathcal{D}_{P_0}$, classified by the class of $[P_0 - P_1]$ in $\mathcal{J}(K)/2\mathcal{J}(K)$. Since, by the Mordell–Weil theorem, $\mathcal{J}(K)$ is finitely generated, we only need a finite number of twists of $\mathcal{D}_{P_0}$ to cover all rational points of $\mathcal{C}(K)$ (this is a special case of [Wet97, Theorem 2.3.3]). Thus, the problem of determining the rational points of a genus 2 curve is transformed to finding the rational points on several curves of genus 17. This would not be progress if we did not have some additional structure.

The involution $[\hat{P}_0 - P_0] \circ [-1]$ can be pulled back under $[2]$ to $\tau_{T_i} = [-1] + [T_i - P_0]$. Note that $\mathcal{D}_{P_0}$ comes equipped with a degree 32 cover of $\mathbb{P}_1$, namely $X \circ [2]$. This $\mathbb{P}_1$ corresponds to $\langle \mathcal{J}[2], \tau_{T_6}\rangle \backslash \mathcal{D}_{P_0}$. By factoring out subgroups of involutions, we get intermediate covers. For instance, take $H_{T_{56}} = \langle T_{12}, T_{13}, T_{14}, \tau_{T_6}\rangle$. It is straightforward to check that τ_{T_5} is also in this group and that $T_{15} \notin H_{T_{56}}$. Put $\mathcal{E}_{P_0} = \mathcal{E}_{P_0,T_{56}} = H_{T_{56}} \backslash \mathcal{D}_{P_0}$. It follows that T_{15} induces a non-trivial involution on $\mathcal{E}_{P_0}$ and that the quotient is $\langle \hat{.} \rangle \backslash \mathcal{C}$. This gives a double cover $\varphi : \mathcal{E}_{P_0} \to \mathbb{P}_1$.

$$
\begin{tikzcd}
 & \mathcal{D}_{P_0} \arrow[dl, "H_{T_{56}}\backslash\cdot"', "\pi"] \arrow[d, "H'_{T_{56}}\backslash\cdot"] \arrow[dr, "\mathcal{J}[2]\backslash\cdot", "{[2]}"'] & \\
\mathcal{E}_{P_0,T_{56}} \arrow[dr, "\varphi", "\langle T_{15}\rangle\backslash\cdot"'] & \mathcal{Q}_{P_0,T_{56}} \arrow[d, "\varphi'"', "\langle T_{15}\rangle\backslash\cdot"] & \mathcal{C}_{P_0} \arrow[dl, "X"', "\langle [-1]+[\hat{P}_0 - P_0]\rangle\backslash\cdot"] \\
 & \mathbb{P}_1 &
\end{tikzcd}
$$

To determine the genus of $\mathcal{E}_{P_0}$, we look at the ramification of this double cover. It can only be ramified above the t_i's. We have that $\varphi^{-1}(\{t_i\}) = H_{T_{56}} \backslash (X \circ [2])^{-1}(\{t_i\})$. If $2D = [T_i - P_0]$, then $\tau_{T_6}(D) = D + T_{i6}$. So, for $i = 1, 2, 3, 4$ we see that $H_{T_{56}}$ works transitively on the fibre. Therefore, φ is ramified above $t_1, \ldots t_4$. By Riemann–Hurwitz, $\mathcal{E}_{P_0}$ is of genus 1.

Note that we can only guarantee that $\mathcal{E}_{P_0}$ is defined over $L = K(T_{56})$ and that $\pi(\mathcal{D}_{P_0}(K)) \subset \mathcal{E}_{P_0}(L)$. However, since φ comes from factoring $X \circ [2]$, which is defined over K, we know that such points map to K-rational points under φ. Thus, we are interested in determining the set $\mathbb{P}_1(K) \cap \varphi(\mathcal{E}_{P_0}(L))$. Taking X^{-1} of this set gives a superset of $C_{P_0}(K) \cap [2](\mathcal{D}_{P_0}(K))$.

In order to make this procedure effective, we have to determine which twists of $\mathcal{E}_{P_0}$ we need. The ramification information of φ completely determines the geometry of $\mathcal{E}_{P_0}$. A double cover of the projective line, ramified above t_1, t_2, t_3, t_4 is of the form

$$\mathcal{E}_\delta : \delta Y_1^2 = R_{T_{56}}(X) = (X - t_1)(X - t_2)(X - t_3)(X - t_4).$$

where $\delta = \delta_{P_0}$ represents an element of $L^*/(L^*)^2$, depending on P_0. We can identify $X : \mathcal{E}_\delta \to \mathbb{P}_1$ with φ.

If we repeat this procedure with $H'_{T_{56}} = \langle T_{12}, T_{13}, T_{14}, \tau_{T_1} \rangle$, we get a double cover of $\mathbb{P}_1$ that is ramified above t_5, t_6. By Riemann–Hurwitz, it is of genus 0 and has a model of the form

$$\mathcal{Q}_{\delta'} : \delta' Y_2^2 = Q_{T_{56}}(X) = f_6(X - t_5)(X - t_6).$$

Again, $X : \mathcal{Q}_{\delta'} \to \mathbb{P}_1$ is the double cover of $\mathbb{P}_1$ induced by $X \circ [2]$ on $\mathcal{D}_{P_0}$.

Note that $F(X) = Q_{T_{56}}(X) R_{T_{56}}(X)$, so for a point $P \in \mathcal{C}(K)$ covered by $\mathcal{D}_{P_0}(K)$ we have a $\delta = \delta_{P_0}$ and a pair of points $(X(P), Y_1) \in \mathcal{E}_\delta(L)$ and $(X(P), Y_2) \in \mathcal{Q}_{\delta'}(L)$ with $Y(P)^2 = \delta\delta' Y_1^2 Y_2^2$. It follows that if $\mathcal{D}_{P_0}(K)$ is non-empty, then δ' should represent the same class as δ_{P_0}. So without loss of generality, we can put $\delta' = \delta_{P_0}$ and we have $Y(P) = \pm\delta Y_1 Y_2$.

The point P_0 is certainly covered by $\mathcal{D}_{P_0}(K)$. Therefore, δ_{P_0} should represent the quadratic class of $R_{T_{56}}(X(P_0))$. For $X(P_0) \in \{t_1, \ldots, t_4\}$, we can determine δ_{P_0} by noticing that δ_{P_0} should also represent the quadratic class of $Q_{T_{56}}(X(P_0))$. It follows that δ_{P_0} will be a square locally at primes where $\operatorname{disc}(F)$ is a unit. Therefore δ_{P_0} is a representative of the finite set $L(S, 2)$, where S is the set of primes dividing $\operatorname{disc}(F)$.

Twists of $\mathcal{E}_\delta$ that have points that correspond to K-rational points of $\mathcal{C}$ are called *productive*. To narrow down the number of $\mathcal{E}_\delta$ that might be productive, we can proceed in the following manner. We let δ run through a set of representatives of $L(S, 2)$, choose a prime p of K together with a prime $\mathfrak{p} \mid p$ of L and see whether there exist $X \in K_p$ such that $R_{T_{56}}(X), Q_{T_{56}}(X) \in \delta \cdot (L_{\mathfrak{p}}^*)^2 \cup \{0\}$. If representatives of $\mathcal{J}(K)/2\mathcal{J}(K)$ are available, then they can give information that helps to reduce the number of candidates for δ as well.

Now we are again in the situation where we have a finite number of degree 2 elliptic covers $\varphi : E \to \mathbb{P}^1$ over a number field L such that for any point $P \in \mathcal{C}(K)$ there is one such cover and a point $G \in E(L)$ such that $\varphi(G) = X(P)$. We are thus led to determine the L-rational points of E with K-rational image under φ. This is discussed in [Bru99b].

3 The equation $x^8 + y^3 = z^2$

In this section we apply the covering techniques to certain curves of genus 2 arising from determining the primitive solutions to the equation $x^8 + y^3 = z^2$. We refer to Table 1 for algebraic number theoretic data and notational conventions used throughout this section.

Our strategy is the following. First we consider the equation $u^4 + y^3 = z^2$. All primitive solutions to this equation can be obtained by specialisation of one of finitely many polynomial solutions to that equation. See [DG95], [Beu98] and [Bru99a] for more information. This gives us that the value of u is a specialisation of one of finitely many degree 6 forms in variables s, t.

For such a solution to correspond to a primitive solution to $x^8 + y^3 = z^2$, we should have $x^2 = u$. This gives equations of the form $x^2 = F(s, t)$, where F is a degree 6 form. By putting $Y = x/t^3$ and $X = s/t$, we see that finding the solutions corresponds to finding the rational points on the curve $Y^2 = F(X, 1)$, where solutions with $t = 0$ correspond to points at infinity on the curve.

To find those rational points, we apply the method described in this article. It is worth noting that equations of the form $F(s,t) = x^2$ have been studied before (see for instance [DG95]) and that Theorem 5.1 in [Bru99b] shows that primitive solutions correspond to rational points on finitely many curves. If we apply that theorem to the equations we meet in this section, we get the curves $\mathcal{D}_\delta$ from the previous section.

Lemma 3.1 (Zagier) *Suppose x, y, z are coprime integers such that $x^4 + y^3 = z^2$. Then there are $s, t \in \mathbb{Z}_{\{2,3\}}$ such that one of the relations in Table 2 holds.*

These parametrisations appeared first in print in [Beu98]. See [Bru99a, Section 3.2] for a description of the principles behind the proof.

Lemma 3.2 *Let $x, y, z \in \mathbb{Z}$ be a primitive solution to $x^8 + y^3 = z^2$. Then there is a $\mathcal{C} = \mathcal{C}_i$ from Table 3 with $P \in \mathcal{C}(\mathbb{Q})$ and $t \in \mathbb{Q}$ such that $x = t^3 Y(P)$.*

Proof: Let x, y, z be such a solution. Then, by Lemma 3.1, we have some homogeneous $F \in \mathbb{Z}[S, T]$ of degree 6 as in Table 2 and $s, t \in \mathbb{Q}$ such that $\pm x^2 = F(s,t)$ This leads to a point $P = (s/t, x/t^3)$ on $\pm Y^2 = F(X, 1)$. These curves are given in Table 3. Note that, for the curves $\mathcal{C}_3$ and $\mathcal{C}_4$, we can control the sign of $F(s,t)$ with the sign of t. Therefore, we only need one of $\pm Y^2 = F(X, 1)$. The curves $\mathcal{C}_9$ and $\mathcal{C}_{10}$ have undergone a small transformation to make $F(X, 1)$ monic. $\square$

For most of these curves, arguments using elliptic curves over $\mathbb{Q}$ suffice. For $\mathcal{C}_5$, $\mathcal{C}_7$ and $\mathcal{C}_9$ we need Section 2. The following lemma establishes the elliptic covers we need to consider. The models given in the lemma follow naturally from the models of the $\mathcal{C}_i$, whereas the models given in Table 4 are in twisted Weierstrass form and therefore are more suitable for computational purposes.

Lemma 3.3 *The $\mathbb{Q}$-rational points on $\mathcal{C}_5$, $\mathcal{C}_7$ and $\mathcal{C}_9$ correspond to L-rational points G on the genus 1 covers $\varphi = X : \mathcal{E}_j \to \mathbb{P}_1$ with $\varphi(G) \in \mathbb{P}_1(\mathbb{Q})$. The following choices for $\mathcal{E}_j$ and L suffice:*

$\mathcal{C}_j$	L	$\mathcal{E}_j$
$\mathcal{C}_5$	$\mathbb{Q}(\beta)$	$\mathcal{E}_5 : Y^2 = X^4 - 2\beta X^3 + 6\beta^2 X^2 + 8X + 8\beta$
$\mathcal{C}_7$	$\mathbb{Q}(\alpha)$	$\mathcal{E}_7 : Y^2 = (X^2 + [2,-2,-2,0,0,-4,0,0,2,2,0,0]X + [-1,0,0,0,0,2,0,0,0,0,0,0])\cdot$
		$(X^2 + [2,0,0,-1,1,3,1,0,-2,0,-1,-3]X + [-1,0,4,3,5,-1,1,2,0,0,-1,-1])$
$\mathcal{C}_9$	$\mathbb{Q}(\alpha)$	$\mathcal{E}_9 : Y^2 = (X^2 + [-2,2,2,0,0,0,0,0,-2,-2,0,0]X + [3,0,0,0,0,6,0,0,0,0,0,0])\cdot$
		$(X^2 + [-2,-2,0,-1,-1,1,-3,-2,0,2,-3,1]X + [3,12,6,3,3,-9,9,0,0,0,-3,3])$

These covers are birational to the ones given in Table 4 with given maps φ.

Proof: Let $\mathcal{C} : Y^2 = F(X)$ be a hyperelliptic model of the genus 2 curve we consider. Let L be an extension of $\mathbb{Q}$ such that $F = R \cdot Q$ with $R, Q \in L[X]$. If $(x, y) \in \mathcal{C}(\mathbb{Q})$, then there are $\delta, y_1, y_2 \in L$ such that $R(x) = \delta y_1^2$ and $Q(x) = \delta y_2^2$. Without loss of generality, we can take δ square-free S-unit, where S contains the places dividing $2\mathrm{disc}(F)$. We then see for which of those δ there exist $x \in \mathbb{Q}$ such that $\delta R(x)$ and $\delta Q(x)$ are squares simultaneously, everywhere locally. As it turns out, in all three cases, this only happens for $\delta = 1$. Note that for $\mathcal{C}_7$ and $\mathcal{C}_9$, we can also find R and Q over $\mathbb{Q}(\beta)$ but the resulting elliptic curves turn out to have rank 3, which means that the described methods cannot be applied. Checking that the covers in Table 4 are indeed birational to the ones mentioned in the lemma is tedious and straightforward. $\square$

We examine the Mordell–Weil groups of the curves in Table 4.

Lemma 3.4 *Let $j = 5, 7, 9$. Consider E_j, G_i, p and M be as given in Tables 4 and 5 and let L be the field of definition of E_j. then the group spanned by the G_i span a subgroup of finite index prime to 2 and p in $E_j(L)$, containing $E_j^{\mathrm{tor}}(L)$. Let $\mathfrak{p}$ be a prime of L above p. Then the reduction of the G_i span $E_j(L) \bmod \mathfrak{p}$. The rows of M form linear combinations of the G_i that span the intersections of the kernels of reduction mod $\mathfrak{p} \mid p$.*

Proof: This lemma is, both in statement and in proof, completely analogous to Lemma 7.7 in [Bru99b]. The ranks can be determined using a 2-isogeny descent (see [Sil86, Proposition X.4.9] or [Bru99a, Section 4.3]). More detailed information and electronic references can be found in [Bru99a, Section 4.8]. $\square$

Proposition 3.5 $\mathcal{C}_1(\mathbb{Q}) = \{\infty^+, \infty^-\}$.

Proof: The curve is a double cover of an elliptic curve by the map $X \mapsto X^2$. The elliptic curve $Y^2 = (X - 3)(X^2 + 18\,X + 9)$ is of rank 0 and has 2 rational points: ∞ and $(3, 0)$. The first is covered by ∞^+ and ∞^-, which are indeed rational points of $\mathcal{C}_1$. The second is covered by $(\pm\sqrt{3}, 0)$, which are quadratic conjugate points. $\square$

Proposition 3.6 $\mathcal{C}_2(\mathbb{Q}) = \emptyset$.

Proof: The curve is a double cover of an elliptic curve by the map $X \mapsto 1/X^2$. The elliptic curve $Y^2 = (3\,X - 1)(9\,X^2 + 18\,X + 1)$ is of rank 0 and has 2 rational points: $(1/3, 0)$ and ∞. Neither of these points lifts to rational points. $\square$

Proposition 3.7 $\mathcal{C}_3(\mathbb{Q}) = \{\infty, (0, 0)\}$.

Proof: We see that for solutions with $X \neq 0, \infty$, we have $X^4 + 12 = \delta\, Y_1^2$ with δ in the set $\{\pm1, \pm2, \pm3, \pm6\}$. It is clear that $\delta \geq 0$ from real considerations and that $2 \nmid \delta$ from considerations locally at 2. Both $X^4 + 12 = Y_1^2$ and $X^4 + 12 = 3\,Y_1^2$ are genus 1 curves of rank 0 with only 2 rational points: the two branches at infinity and the two points with $X = 0$ respectively. $\square$

Proposition 3.8 $\mathcal{C}_4(\mathbb{Q}) = \{\infty, (0, 0)\}$.

Proof: We see that for solutions with $X \neq 0, \infty$, we have $3\,X^4 + 4 = \delta\, Y_1^2$ with δ in the set $\{\pm1, \pm2, \pm3, \pm6\}$. It is clear that $\beta \geq 0$ from real considerations and that $2 \nmid \beta$ from considerations locally at 2. Both $3\,X^4 + 4 = 3\,Y_1^2$ and $3\,X^4 + 4 = Y_1^2$ are genus 1 curves of rank 0 with only 2 rational points: the two branches at infinity and the two points with $X = 0$ respectively. $\square$

Proposition 3.9 $\mathcal{C}_6(\mathbb{Q}) = \mathcal{C}_8(\mathbb{Q}) = \mathcal{C}_{10}(\mathbb{Q}) = \emptyset$.

Proof: It is easy to check that $\mathcal{C}_6(\mathbb{Q}_3) = \emptyset$, $\mathcal{C}_8(\mathbb{Q}_2) = \emptyset$ and $\mathcal{C}_{10}(\mathbb{Q}_3) = \emptyset$. □

Proposition 3.10 *The following statements are true:*

- $\mathcal{C}_5(\mathbb{Q}) = \{\infty^+, \infty^-, (1,3), (1,-3)\}$,
- $\mathcal{C}_7(\mathbb{Q}) = \{\infty^\pm, (1/2, \pm 15/8)\}$,
- $\mathcal{C}_9(\mathbb{Q}) = \{\infty^\pm, (9/2, \pm 387/8)\}$.

Proof: Using Lemma 3.3, we reduce these statements to proving that

$$\begin{aligned} \varphi_5(E_5(\mathbb{Q}(\beta))) \cap \mathbb{P}_1(\mathbb{Q}) &= \{0, 1, \infty\}, \\ \varphi_7(E_7(\mathbb{Q}(\alpha))) \cap \mathbb{P}_1(\mathbb{Q}) &= \{\tfrac{1}{2}, \infty\}, \\ \varphi_9(E_9(\mathbb{Q}(\alpha))) \cap \mathbb{P}_1(\mathbb{Q}) &= \{\tfrac{9}{2}, \infty\}. \end{aligned}$$

where one should note that $X = 0$ on $\mathcal{C}_5$ does not lead to a rational point. These statements are of exactly the same form as those in [Bru99b, Proposition 7.11] and can be proved along exactly the same lines. Table 6 contains the essential data. We refer to [Bru99a] and the electronic references given there for details. □

Proof of Theorem 1.1 We now complete our proof by checking to which solutions the rational points on $\mathcal{C}_1, \ldots, \mathcal{C}_{10}$ correspond. Since at least one of the forms for x, y, z in Lemma 3.1, corresponding to $\mathcal{C}_1, \ldots, \mathcal{C}_6$, is divisible by s and t, points with $X = 0, \infty$ correspond to solutions with $xyz = 0$. This only leaves $(1, \pm 3)$ on $\mathcal{C}_5$. The corresponding solutions are $(x, y, z) = (\pm 3, 2^3 \cdot 3^2 \cdot 5, \pm 3^3 \cdot 11 \cdot 23)$. Being a remarkable relation in itself, it does not satisfy the condition that $(x, y, z) = 1$. Furthermore, it cannot be transformed into such a solution using a weighted multiplication $(x, y, z) \mapsto (\lambda^3 x, \lambda^8 y, \lambda^{12} z)$ either.

On $\mathcal{C}_7$, the points $\infty^\pm$ correspond to $(\pm 1, 2, \pm 3)$ and the points $(1/2, \pm 15/8)$ correspond (after clearing denominators) to $(\pm 3 \cdot 5, 2 \cdot 3^2 \cdot 29 \cdot 37, \pm 3^3 \cdot 99431)$. On $\mathcal{C}_9$, $\infty^\pm$ correspond to $(\pm 3, -2 \cdot 3^2, \pm 3^3)$ and $(9/2, \pm 387/8)$ (after clearing denominators) to $(\pm 43, 2 \cdot 3 \cdot 7 \cdot 29 \cdot 79, \pm 109 \cdot 275623)$. We conclude that the list stated in the theorem is complete. □

References

[Beu98] Frits Beukers. The Diophantine equation $Ax^p + By^q = Cz^r$. *Duke Math. J.*, 91:61–88, 1998.

[Bru97] Nils Bruin. The diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$. Technical Report W97-21, University of Leiden, 1997. To appear in Compositio Math.

[Bru99a] Nils Bruin. *Chabauty methods and covering techniques applied to generalised Fermat equations.* PhD thesis, University of Leiden, 1999.

[Bru99b] Nils Bruin. Chabauty methods using elliptic curves. Technical Report W99-14, University of Leiden, 1999.

[CF96] 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.

[Cha41] Claude Chabauty. Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension. *C. R. Acad. Sci. Paris*, 212:1022–1024, 1941.

[DG95] Henri Darmon and Andrew Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27:513–543, 1995.

[Fly97] E.V. Flynn. A flexible method for applying Chabauty's theorem. *Compositio Math.*, 105:79–94, 1997.

[FPS97] E. V. Flynn, Bjorn Poonen, and Edward F. Schaefer. Cycles of quadratic polynomials and rational points on a genus-2 curve. *Duke Math. J.*, 90:435–463, 1997.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. GTM 106. Springer-Verlag, 1986.

[Wet97] Joseph L. Wetherell. *Bounding the number of rational points on certain curves of high rank*. PhD thesis, U.C. Berkeley, 1997.

Address for correspondence: Nils Bruin, Math. Institute, Leiden University, P.O. Box 9512, 2300 RA Leiden, The Netherlands; e-mail: nbruin@wi.leidenuniv.nl

$$\beta^3 - 2 = 0\,; \quad \alpha^{12} + 6\alpha^{10} + 39\alpha^8 + 64\alpha^6 + 15\alpha^4 - 6\alpha^2 - 3 = 0$$

L	$\mathbb{Z}$ basis of $\mathcal{O}_L$	$\mathrm{disc}(\mathcal{O}_L/\mathbb{Z})$	$\mathcal{O}_L^*$	$\mathrm{reg}(\mathcal{O}_L^*)$	$h(\mathcal{O}_L)$
$\mathbb{Q}(\beta)$	$1, \beta, \beta^2$	-108	$\langle -1, 1-\beta \rangle$	1.3474	1
$\mathbb{Q}(\alpha)$	$b_1, \ldots, b_{12}$	$-2^{26}3^{13}$	$\langle -1, \eta_1, \ldots, \eta_6 \rangle$	321.19	1

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \\ b_9 \\ b_{10} \\ b_{11} \\ b_{12} \end{pmatrix}^T = \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \\ \alpha^4 \\ \alpha^5 \\ \alpha^6 \\ \alpha^7 \\ \alpha^8 \\ \alpha^9 \\ \alpha^{10} \\ \alpha^{11} \end{pmatrix}^T \begin{pmatrix} 1 & 0 & -1 & 0 & -7 & 0 & 49 & 0 & 33 & 0 & -1641 & 0 \\ 0 & 0 & 1 & 0 & 1 & 8 & -28 & -38 & 66 & -88 & 613 & 1496 \\ 0 & 0 & -1 & -4 & 5 & 17 & 24 & 47 & -270 & -692 & 379 & 1290 \\ 0 & 1 & 0 & 0 & 0 & -27 & 0 & 96 & 0 & 455 & 0 & -4742 \\ 0 & 0 & 0 & -1 & 8 & 1 & -38 & 30 & -88 & -158 & 1496 & -273 \\ 0 & 0 & 0 & 0 & -7 & -8 & 33 & 38 & 64 & 88 & -1226 & -1496 \\ 0 & 0 & 0 & 3 & 0 & -8 & 0 & -55 & 0 & 446 & 0 & -67 \\ 0 & 0 & 0 & -4 & 0 & -2 & 0 & 150 & 0 & -564 & 0 & -2276 \\ 0 & 0 & 1 & 1 & -1 & -16 & -30 & 41 & 158 & 310 & 273 & -2449 \\ 0 & 0 & 1 & -1 & -1 & 16 & -30 & -41 & 158 & -310 & 273 & 2449 \\ 0 & 0 & 0 & 1 & 0 & -12 & 0 & 35 & 0 & 198 & 0 & -1797 \\ 0 & 0 & 0 & -3 & 0 & 24 & 0 & -21 & 0 & -622 & 0 & 3059 \end{pmatrix}^{-1}$$

Elements of $\mathbb{Q}(\alpha)$ are given with respect to the basis $b_1, \ldots, b_{12}$.

$\eta_1 = [0,1,0,0,0,0,0,0,0,0,0,0]$	$\eta_2 = [0,1,0,0,0,0,1,0,-1,0,0,0]$
$\eta_3 = [0,0,1,0,1,0,0,0,0,0,-1,0]$	$\eta_4 = [0,0,0,0,0,0,0,0,0,0,1,0]$
$\eta_5 = [0,-1,-1,0,0,0,0,1,1,0,1,-1]$	$\eta_6 = [0,1,-1,0,0,0,1,-1,0,0,0,0]$

L	p	$\mathfrak{p}$	defining relation	$\mathbb{F}_p$-basis of $\mathcal{O}/\mathfrak{p}$
$\mathbb{Q}(\beta)$	2	$\mathfrak{p}_2$	$\mathfrak{p}_2 = \beta\mathcal{O}\,;\ 2\mathcal{O} = \mathfrak{p}_2^3$	
	3	$\mathfrak{p}_3$	$\mathfrak{p}_3 = (1+\beta)\mathcal{O}\,;\ 3\mathcal{O} = \mathfrak{p}_3^3$	
	5	$\mathfrak{p}_{5,1}$	$\beta + 2 \bmod \mathfrak{p}_{5,1} = 0$	1
		$\mathfrak{p}_{5,2}$	$\beta^2 - 2\beta - 1 \bmod \mathfrak{p}_{5,2} = 0$	$1, \beta$
$\mathbb{Q}(\alpha)$	2	$\mathfrak{p}_2$	$\mathfrak{p}_2 = [0,1,0,0,1,0,1,0,0,0,0,0]\mathcal{O}\,;\ 2\mathcal{O} = \mathfrak{p}_2^{12}$	
	3	$\mathfrak{p}_3$	$\mathfrak{p}_3 = [1,0,1,0,0,0,0,0,0,0,-1,0]\mathcal{O}$	
		$\mathfrak{q}_3$	$\mathfrak{q}_3 = [1,0,0,0,0,-1,0,0,1,1,0,0]\mathcal{O}\,;\ 3\mathcal{O} = \mathfrak{p}_3^6\mathfrak{q}_3^3$	
	31	$\mathfrak{p}_{31,1}$	$\alpha - 5 \bmod \mathfrak{p}_{31,1} = 0$	1
		$\mathfrak{p}_{31,2}$	$\alpha + 12 \bmod \mathfrak{p}_{31,2} = 0$	1
		$\mathfrak{p}_{31,3}$	$\alpha + 5 \bmod \mathfrak{p}_{31,3} = 0$	1
		$\mathfrak{p}_{31,4}$	$\alpha - 12 \bmod \mathfrak{p}_{31,4} = 0$	1
		$\mathfrak{p}_{31,5}$	$\alpha^2 - 5\alpha + 13 \bmod \mathfrak{p}_{31,5} = 0$	$1, b_2$

Table 1: Data regarding number fields

$$\begin{aligned}
\pm x &= (s^2-3\,t^2)(s^4+18\,t^2s^2+9\,t^4)\\
y &= -(s^2+2\,ts+3\,t^2)(s^2-2\,ts+3\,t^2)(s^2+6\,ts+3\,t^2)(s^2-6\,ts+3\,t^2)\\
\pm z &= 4\,st(s^2+3\,t^2)(3\,s^4-2\,t^2s^2+3\,t^4)(s^4-6\,t^2s^2+81\,t^4)
\end{aligned}$$

$$\begin{aligned}
\pm x &= 6\,st(s^4+12\,t^4)\\
y &= (s^4-12\,t^2s^2-12\,t^4)(s^4+12\,t^2s^2-12\,t^4)\\
\pm z &= (s^4-12\,t^4)(s^8+408\,t^4s^4+144\,t^8)
\end{aligned}$$

$$\begin{aligned}
\pm x &= 6\,st(3\,s^4+4\,t^4)\\
y &= (3\,s^4+12\,t^2s^2-4\,t^4)(3\,s^4-12\,t^2s^2-4\,t^4)\\
\pm z &= (3\,s^4-4\,t^4)(9\,s^8+408\,t^4s^4+16\,t^8)
\end{aligned}$$

$$\begin{aligned}
\pm x &= s^6+40\,t^3s^3-32\,t^6\\
y &= -8\,t\,s(s^3-16\,t^3)(s^3+2\,t^3)\\
\pm z &= (s^6+32\,t^6)(s^6-176\,t^3s^3-32\,t^6)
\end{aligned}$$

$$\begin{aligned}
\pm x &= s^6+6\,s^5t-15\,s^4t^2+20\,t^3s^3+15\,s^2t^4+30\,st^5-17\,t^6\\
y &= 2\,(s^4-4\,ts^3-6\,t^2s^2+4\,t^3s-7\,t^4)(s^4+6\,t^2s^2-8\,t^3s-3\,t^4)\\
\pm z &= 3\,s^{12}-12\,ts^{11}+66\,t^2s^{10}+44\,t^3s^9-99\,t^4s^8-792\,t^5s^7+924\,t^6s^6\\
&\quad -2376\,t^7s^5+1485\,t^8s^4+1188\,t^9s^3-2046\,t^{10}s^2+156\,t^{11}s-397\,t^{12}
\end{aligned}$$

$$\begin{aligned}
\pm x &= 9\,s^6-18\,ts^5+45\,t^2s^4-60\,t^3s^3+15\,t^4s^2+6\,t^5s-5\,t^6\\
y &= -2\,(3\,s^4-6\,t^2s^2+8\,t^3s-t^4)(3\,s^4-12\,ts^3+6\,t^2s^2-4\,t^3s+3\,t^4)\\
\pm z &= 27\,s^{12}+324\,ts^{11}-1782\,t^2s^{10}+3564\,t^3s^9-3267\,t^4s^8+2376\,t^5s^7-2772\,t^6s^6\\
&\quad +3960\,t^7s^5-4059\,t^8s^4+2420\,t^9s^3-726\,t^{10}s^2+156\,t^{11}s-29\,t^{12}
\end{aligned}$$

Table 2: Parametrisations of $x^4+y^3=z^2$

$$\begin{aligned}
\mathcal{C}_1 &: Y^2=(X^2-3)(X^4+18\,X^2+9)\\
\mathcal{C}_2 &: Y^2=-(X^2-3)(X^4+18\,X^2+9)\\
\mathcal{C}_3 &: Y^2=6X(X^4+12)\\
\mathcal{C}_4 &: Y^2=6X(3X^4+4)\\
\mathcal{C}_5 &: Y^2=X^6+40X^3-32\\
\mathcal{C}_6 &: Y^2=-X^6-40X^3+32\\
\mathcal{C}_7 &: Y^2=X^6+6\,X^5-15\,X^4+20\,X^3+15\,X^2+30\,X-17\\
\mathcal{C}_8 &: Y^2=-X^6-6\,X^5+15\,X^4-20\,X^3-15\,X^2-30\,X+17\\
\mathcal{C}_9 &: Y^2=X^6-6\,X^5+45\,X^4-180\,X^3+135\,X^2+162\,X-405\\
\mathcal{C}_{10} &: Y^2=-X^6+6\,X^5-45\,X^4+180\,X^3-135\,X^2-162\,X+405
\end{aligned}$$

Table 3: Parametrising curves for $x^8+y^3=z^2$

j	E_j	c
5	$-6Y^2 = X^3 - X$	$\begin{pmatrix} \beta & -6\beta & \beta \\ 2 & 0 & -1 \end{pmatrix}$
7	$[0,0,0,-1,-1,0,-1,0,0,0,1,0]Y^2 = X^3 + 2X^2 + 2X$	C_7
9	$[0,0,0,1,1,-1,1,1,0,-1,1,-1]Y^2 = X^3 + 2X^2 + 2X$	C_9

$$C_7 = \begin{pmatrix} [4,-4,-4,-2,0,6,-2,8,4,-6,10,-8] & -12 & [2,1,2,5,2,-2,1,0,1,-3,-1,-3] \\ [0,4,0,4,0,0,0,-4,4,0,0,4] & 0 & [4,-3,0,5,2,-8,-1,-4,3,5,-5,5] \end{pmatrix}$$

$$C_9 = \begin{pmatrix} [0,2,6,0,-6,10,-10,6,-2,-10,2,2] & -12 & [0,7,2,1,-2,2,-3,2,1,-7,3,-1] \\ [-4,0,0,0,-4,0,0,0,0,-4,4,4] & 0 & [0,3,2,-1,0,2,-1,0,-1,-3,1,-1] \end{pmatrix}$$

$$\varphi(X,Y) = \frac{c_{11}X + c_{12}Y + c_{13}}{c_{21}X + c_{22}Y + c_{23}}$$

j	G_i
5	$(-2,1)$
	$((-4-2\beta-\beta^2)/6, (1+\beta^2)/6)$
	$(1,0)$
	$(0,0)$
7	$([0,-1,6,-4,0,-1,-2,0,-4,0,-1,4], [8,-2,23,-12,-2,0,-6,7,-18,0,-6,14])$
	$([-1,-1,0,0,0,1,-1,1,0,0,0,-1], [0,0,0,1,1,-1,1,0,0,0,-1,-1])$
	$([1,0,0,-1,0,0,1,-1,-1,1,0,-1], [0,0,0,2,0,2,0,0,0,-4,0,-2])$
	$([-11,-1,-7,-2,-3,-10,0,-1,5,3,3,2]/12, -[4,-5,5,0,3,6,-10,4,-2,1,-5,1]/12)$
	$(0,0)$
9	$([1,-2,-4,-1,0,2,-1,1,1,1,2,-3]/3, [-4,-2,0,0,0,2,4,-2,-4,2,0,4]/3)$
	$([-7,1,-12,2,-2,2,2,-5,2,2,5,-6]/3, [28,-6,16,36,-2,-6,2,26,30,-12,-12,2]/3)$
	$([-1,2,0,0,-1,-2,1,-1,-1,1,0,1], [0,-4,-2,-1,-5,1,-5,2,4,-2,5,-1])$
	$([1,5,-3,-2,-1,-4,0,-7,-3,7,-5,6]/4, [5,2,-4,0,0,1,6,2,3,-6,5,-5]/4])$
	$(0,0)$

Table 4: Weierstrass models of covers and Mordell–Weil pseudo-generators

j	p	M	$Z(B)/p \bmod p$
5	5	$\begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 4 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 4 & 4 \\ 4 & 1+4\beta \end{pmatrix}$
7	31	$\begin{pmatrix} 16 & 0 & 0 & 8 & 1 \\ 0 & 16 & 0 & 8 & 0 \\ 0 & 0 & 32 & 0 & 0 \\ 0 & 0 & 0 & 16 & 0 \end{pmatrix}$	$\begin{pmatrix} 23 & 21 & 1 & 19 \\ 12 & 30 & 28 & 21 \\ 21 & 11 & 4 & 20 \\ 26 & 27 & 25 & 30 \\ 23\alpha+7 & 11+\alpha & 22\alpha+1 & 19\alpha+8 \end{pmatrix}$
9	31	$\begin{pmatrix} 4 & 4 & 368 & 88 & 0 \\ 0 & 32 & 320 & 16 & 0 \\ 0 & 0 & 480 & 0 & 0 \\ 0 & 0 & 0 & 240 & 0 \end{pmatrix}$	$\begin{pmatrix} 25 & 4 & 17 & 29 \\ 27 & 4 & 28 & 29 \\ 12 & 23 & 26 & 0 \\ 7 & 15 & 17 & 13 \\ 11\alpha+13 & 21+8\alpha & 17\alpha+23 & 19\alpha+25 \end{pmatrix}$

For E_7 and E_9, only $\bigcap_{k=1}^{5}(E(L) \cap E^{(1)}(L_{\mathfrak{p}_{31,k}}))$ is considered.

Table 5: kernels of reduction

j	G	$\varphi(G)$	$\theta^G(n_1,\dots,n_r)$
5	∞	∞	$5\begin{pmatrix} 2n_1+2n_2 \\ 2n_1+3n_2 \end{pmatrix} \bmod 5^2$
	G_3-G_1	0	$5\begin{pmatrix} 3n_1+2n_2 \\ 4n_1+4n_2 \end{pmatrix} \bmod 5^2$
	G_2	1	$5\begin{pmatrix} 4n_1+0n_2 \\ n_1+n_2 \end{pmatrix} \bmod 5^2$
7	∞	∞	$31\begin{pmatrix} 13 & 0 & 0 & 24 \\ 4 & 4 & 4 & 21 \\ 13 & 19 & 23 & 24 \\ 20 & 16 & 11 & 1 \\ 30 & 15 & 18 & 28 \end{pmatrix}\begin{pmatrix} n_1 \\ n_2 \\ n_3 \\ n_4 \end{pmatrix} \bmod 31^2$
	G_4	$\frac{1}{2}$	$31\begin{pmatrix} 30 & 20 & 29 & 26 \\ 24 & 15 & 18 & 13 \\ 21 & 18 & 1 & 18 \\ 27 & 26 & 4 & 3 \\ 6 & 0 & 21 & 17 \end{pmatrix}\begin{pmatrix} n_1 \\ n_2 \\ n_3 \\ n_4 \end{pmatrix} \bmod 31^2$
9	∞	∞	$31\begin{pmatrix} 16 & 24 & 16 & 19 \\ 26 & 24 & 4 & 9 \\ 29 & 4 & 28 & 26 \\ 26 & 5 & 13 & 23 \\ 4 & 23 & 11 & 15 \end{pmatrix}\begin{pmatrix} n_1 \\ n_2 \\ n_3 \\ n_4 \end{pmatrix} \bmod 31^2$
	$-G_4$	$\frac{9}{2}$	$31\begin{pmatrix} 28 & 14 & 19 & 24 \\ 18 & 19 & 29 & 11 \\ 0 & 18 & 19 & 25 \\ 15 & 29 & 17 & 6 \\ 30 & 28 & 24 & 9 \end{pmatrix}\begin{pmatrix} n_1 \\ n_2 \\ n_3 \\ n_4 \end{pmatrix} \bmod 31^2$

Table 6: Fibres of rational points