JOURNAL OF NUMBER THEORY 36, 257–265 (1990)

Large Rational Torsion on Abelian Varieties

E. V. FLYNN

University of Michigan, Ann Arbor, Michigan 48109

Communicated by D. J. Lewis

Received November 19, 1989; revised January 2, 1990

A method of searching for large rational torsion on Abelian varieties is described. A few explicit applications of this method over $\mathbb{Q}$ give rational 11- and 13-torsion in dimension 2, and rational 29-torsion in dimension 4.

INTRODUCTION

The search for large rational torsion on elliptic curves goes back to the early 1900s, when Levi [6], Billing and Mahler [1], and others found, for various values of N, the curve $X_1(N)$ whose rational points correspond to elliptic curves with rational N-torsion. These authors found rational points of order 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 12 on elliptic curves over $\mathbb{Q}$, and proved the non-existence of various torsions. It follows from Mazur's result in [7] that no others may occur.

The search for large rational torsion on Abelian varieties in theory entails finding rational points on associated higher dimensional varieties which are analogous to the $X_1(N)$. In practice, it soon becomes apparent that the equations defining these varieties are far too large to be dealt with directly; we shall describe a technique which exploits additions of a certain simple type to obtain manageable subvarieties, on which rational points may more easily be sought. This method will be illustrated in Section 3, in which new torsions over $\mathbb{Q}$ are found.

1. PRELIMINARY DEFINITIONS

We shall work over a perfect ground field K, and employ the following notation (after [9, Chap. 1]). Let $\bar{K}$ denote the algebraic closure of K and $G_{\bar{K}/K}$ the Galois group of $\bar{K}$ over K. Given a smooth curve $\mathscr{C}$ over K, let $\mathrm{Div}(\mathscr{C})$ denote the free Abelian group generated by the points of $\mathscr{C}$ over $\bar{K}$.

0022-314X/90 $3.00

Thus a divisor $D \in \mathrm{Div}(\mathscr{C})$ is a formal sum

$$D = \sum_{P \in C} n_P(P)$$

with $n_P \in \mathbb{Z}$, and $n_P = 0$ for all but finitely many $P \in \mathscr{C}$. A divisor is *effective* if $n_P \geqslant 0$ for all P. The *degree* of D is defined to be $\sum_{P \in \mathscr{C}} n_P$, and we let $\mathrm{Div}^0(\mathscr{C})$ denote the subgroup of $\mathrm{Div}(\mathscr{C})$ of divisors of degree 0. We further denote the quotients of $\mathrm{Div}(\mathscr{C})$ and $\mathrm{Div}^0(\mathscr{C})$ modulo linear equivalence by $\mathrm{Pic}(\mathscr{C})$ and $\mathrm{Pic}^0(\mathscr{C})$, respectively. Finally, let $\mathrm{Div}_K(\mathscr{C})$, $\mathrm{Div}^0_K(\mathscr{C})$, $\mathrm{Pic}_K(\mathscr{C})$, $\mathrm{Pic}^0_K(\mathscr{C})$ denote the subgroups of these fixed by $G_{\bar{K}/K}$. We wish to find curves $\mathscr{C}$ of genus > 1 for which $\mathrm{Pic}^0_K(\mathscr{C})$ (the Mordell–Weil group over K) has large torsion; in particular, we are interested in those torsions which do not occur for elliptic curves.

We can now introduce a few definitions which are required to describe our searching technique. Note that, although we shall deal with what in theory may be regarded as subvarieties of moduli spaces, no attempt is made to address moduli problems (or to discuss precise conditions when our models provide a unique representation of points on such spaces). Rather, the emphasis will be on providing a practical tool for finding large rational torsions; we shall therefore introduce only the minimum amount of general theory and notation required to motivate the explicit examples of Section 3.

DEFINITION 1.1. Let m be a non-negative integer, and let $K(\mathbf{w}) = K(w_1, ..., w_m)$, where $w_1, ..., w_m$ are algebraically independent. By an *m-parameter system of curves of genus g over K* (or an *(m, g)-system over K*), we shall mean a curve $\mathscr{C}$ of genus g with a model defined over $K(\mathbf{w})$, together with a distinguished divisor class $\mathscr{O} \in \mathrm{Pic}_{K(\mathbf{w})}(\mathscr{C})$ of degree g. We shall denote such a system by $\mathscr{S}_m(\mathscr{C}, \mathscr{O})$, or simply $\mathscr{S}_m$, and shall always take our affine model of $\mathscr{C}/K(\mathbf{w})$ to be in the indeterminates X, Y.

Each equivalence class $\mathscr{D} \in \mathrm{Pic}^0_{K(\mathbf{w})}(\mathscr{C})$ will be represented by an effective divisor D of degree g which lies inside $\mathscr{D} + \mathscr{O}$. We may write any as an unordered set of g points on $\mathscr{C}$: $\{P_1, ..., P_g\} = \{(x_1, y_1), ..., (x_g, y_g)\}$, with multiplicities written out explicitly. Corresponding to such a D is a pair of polynomials $(a_D(x), b_D(x))$, both defined over $K(\mathbf{w})$: $a_D(x) = \prod_{i=1}^{g}(x - x_i)$, $b_D(x) = \sum_{i=1}^{g} y_i \prod_{j \neq i}(x - x_i)/(x_j - x_i)$ (so that each $y_i = b_D(x_i)$).

EXAMPLE 1.2. Consider the curve over $\mathbb{Q}(w_1, ..., w_5)$

$$\mathscr{C}: Y^2 + w_1 Y + w_4 XY = X^2(X^4 + w_5 X^3 + w_3 X^2 + w_2 X + w_1) \qquad (1)$$

which is smooth apart from a singularity at infinity, whose two branches

(both rational) will be denoted by ∞^+ and ∞^-. The above general development (which was stated only for smooth curves) holds perfectly well here, provided that we formally admit ∞^+ and ∞^- as rational points on $\mathscr{C}$. Then $\mathscr{C}$, together with the class $\mathscr{O} = [\infty^+ + \infty^-]$, is a $(5, 2)$-system over $\mathbb{Q}$. Any member of $\mathrm{Pic}^0_{\mathbb{Q}(\mathbf{w})}(\mathscr{C})$ may be written in the form $\{P_1, P_2\} \in \mathscr{C}^{(2)}$, where P_1, P_2 either are both defined over $\mathbb{Q}(\mathbf{w})$ or are quadratic and conjugate over $\mathbb{Q}(\mathbf{w})$. Generically, three such pairs sum to $\mathscr{O}$ if there is a function of the form $Y - \alpha X^3 - \beta X^2 - \gamma X - \delta$ which meets $\mathscr{C}$ at all six component points; this gives an explicit means of computing the group law in $\mathrm{Pic}^0_{\mathbb{Q}(\mathbf{w})}(\mathscr{C})$.

DEFINITION 1.3. Let $\mathscr{S}_m = \mathscr{S}_m(\mathscr{C}, \mathscr{O})$ be as in Definition 1.1, let $D_1 \in \mathrm{Pic}^0_{K(\mathbf{w})}(\mathscr{C})$, and let $\langle D_1 \rangle$ represent the subgroup generated by D_1. A *condition on* D_1 (with respect to $\mathscr{S}_m$) is a relation of the form $R : lD_1 = D_l$, for some integer l, and some $D_l \in \mathrm{Pic}^0_{K(\mathbf{w})}(\mathscr{C})$. Now, equating coefficients of $a_{lD_1}(x)$ with $a_{D_l}(x)$, and $b_{lD_1}(x)$ with $b_{D_l}(x)$ (all of which lie in $K(\mathbf{w})$) gives a model of an algebraic set over K in affine m-space A^m with indeterminates $w_1, \ldots, w_m$. We shall denote this set, together with this model over K, by $V(\mathscr{S}_m, R)$, or the algebraic set *induced by* R. If $\mathscr{R} = \{R_1, \ldots, R_r\} = \{l_1 D_1 = D_{l_1}, \ldots, l_r D_1 = D_{l_r}\}$ is a set of conditions on D_1, we define $V(\mathscr{S}_m, \mathscr{R})$ to be the intersection of the $V(\mathscr{S}_m, R_i)$, $1 \leqslant i \leqslant r$.

The relevance to the search for large rational torsion (as will be outlined in the following section) is that, if the conditions in $\mathscr{R}$ imply $ND_1 = \mathscr{O}$ for some N (and where N is the smallest such), then a K-rational point $\mathbf{w}_0$ on $V(\mathscr{S}_m, \mathscr{R})$ will generally correspond to a curve of genus g over K, together with an N-torsion divisor over K (namely, the specialisations of $\mathscr{C}$ and D_1 to $\mathbf{w}_0$). In order to choose conditions $\mathscr{R}$ which simplify the induced model, it will be crucial to make of the following simple type of addition on the Jacobian.

DEFINITION 1.4. Let $\mathscr{S}_m$ be as in Definition 1.1, and let D_1, D_2 represent members of $\mathrm{Pic}^0_{K(\mathbf{w})}(\mathscr{C})$ (where, as usual, D_1, D_2 are of degree g). The addition $D_1 + D_2$ is *degenerate* (with respect to $\mathscr{S}_m$) if $D_1 + D_2 - o$ is an effective divisor for some $o \in \mathscr{O}$. We observe that, in such a case, we may take $D_1 + D_2 - o$ to represent the sum $D_1 + D_2$ (according to the notation of 1.1), and so the calculation of the sum is dependent only upon D_1, D_2, and $\mathscr{O}$.

EXAMPLE 1.5. Let $\mathscr{C}$, $\mathscr{O}$ be as in Example 1.2. Degenerate additions are then precisely those of the form

$$\{(x_1, y_1), (x_2, y_2)\} + \{(x_2, y_2 - w_1 - w_4 x_2), (x_3, y_3)\}$$

in which case the sum is represented by $\{(x_1, y_1), (x_3, y_3)\}$.

2. A Description of the Method

We shall first state the 'obvious' analogue of the method used classically to search for rational torsion on elliptic curves; this turns out not to be viable. We then sketch the refinement, which will motivate the explicit examples of Section 3.

For elliptic curves, Tate Normal Form may be used (see [8]) to derive models for the curves $X_1(N)$, as follows. One first writes out the (2, 1)-system ($w_2 \neq 0$)

$$\mathscr{E}: Y^2 + (1 - w_1)XY - w_2 Y = X^3 - w_2 X^2$$

together with $\mathcal{O} = \infty$, $D_1 = (0, 0)$. Note that $Y = 0$ is tangent to $\mathscr{E}$ at $(0, 0)$ which eases the calculation of $2D_1$. We then see

$$2D_1 = (w_2, w_1 w_2), \qquad 3D_1 = (w_1, w_2 - w_1),$$
$$4D_1 = (w_2(w_2 - w_1)/w_1^2,\ w_2^2(w_1^2 - w_2 + w_1)/w_1^3),$$

giving (for example) the model in $A^2 : w_1 = w_2$ for $X_1(5)$, induced by $R : 2D_1 = -3D_1$ (that is to say: $(w_2, w_1 w_2) = (w_1, w_1^2)$). Note that it was sufficient to equate the x-coordinates of $2D_1$ and $-3D_1$; equating y-coordinates gives a redundant equation (lying in the variety defined by $w_1 = w_2$). Substituting $w_1 = w_2$ into $\mathscr{E}$ then gives a 1-parameter family of elliptic curves with a rational 5-torsion point (namely (0, 0)).

A direct analogue of this method for general genus is as follows. For a given K, genus g, and desired torsion N, choose an $\mathscr{S}_m$ together with a $D_1 \in \mathrm{Pic}^0_{K(\mathbf{w})}(\mathscr{C})$ (the potential N-torsion divisor), such that $Y = 0$ is tangent to $\mathscr{C}$ at the points on the support of D_1 (this eases the calculation of $2D_1$). Ensure that m (the number of parameters) is at least the size of the moduli space for genus g (which is $3g - 3$, or $2g - 1$ if we restrict our attention to hyperelliptic curves), and that $K(\mathbf{w})$ is generated by the coefficients of the $X^i Y^j$ in the model of $\mathscr{C}$. Let R be the condition: $ND_1 = \mathcal{O}$. Derive the model for $V(\mathscr{S}_m, R)$ in A^m explicitly by first finding ND_1, $a_{ND_1}(x)$, $b_{ND_1}(x)$ explicitly over $K(\mathbf{w})$. Finally, find a rational point on $V(\mathscr{S}_m, R)$. A slight computational improvement may be obtained (as with the elliptic curve example above) by using the condition $\lfloor N/2 \rfloor D_1 = -\lfloor (N+1)/2 \rfloor D_1$ rather than $ND_1 = \mathcal{O}$ (where $\lfloor\ \rfloor$ denotes integer part). As we shall soon restrict our attention to small-dimensional subvarieties of $V(\mathscr{S}_m, R)$ (from the point of view of searching for rational points, rather than proving the non-existence of given rational torsions), we fortunately need not concern ourselves with such subtleties as the precise conditions on $\mathscr{S}_m$ such that $V(\mathscr{S}_m, R)$ gives a *complete* parametrisation over K of genus g curves $/K$ with K-rational N-torsion. It will become apparent that the overriding consideration is that of working with manageably small defining equations.

This approach for genus $g>1$ becomes quickly unviable at the stage of finding ND_1 (or $[(N+1)/2]\,D_1$) explicitly over $K(\mathbf{w})$. Whatever method one uses for computing the group law on the Jacobian (see, for example, [2, 3, 5]), one finds that the expressions over $K(\mathbf{w})$ (that is, rational functions in $w_1, \ldots, w_m$ over K) for ND_1 become far too large to handle for $N>5$. For example, in the $(5, 2)$-system of Example 1.2, with $D_1 = \{(0, 0), \infty^+\}$, the rational functions in $w_1 \cdots w_5$ over $\mathbb{Q}$ defining $7D_1$ were too large to be held in 6 Mbytes of storage. We therefore introduce the following refinement.

METHOD 2.1. For a given K, genus g, and desired torsion N, we let $\mathscr{S}_m$ and D_1 be as above. However, we now take $\mathscr{R}$ to be a *larger* set of conditions on D_1, which imply $ND_1 = \mathcal{O}$ (and for which N is the smallest such). We first restrict the size of $\mathscr{R}$ by requiring that $V(\mathscr{S}_m, \mathscr{R})$ must have dimension at least 1. We then give preference to those $\mathscr{R}$ which maximise the number of:

— degenerate additions which occur in $\langle D_1 \rangle$, and

— w_i's which are linear in $V(\mathscr{S}_m, R)$.

The first property greatly simplifies the expressions over $K(\mathbf{w})$ for the multiples lD_1, and makes the second property more likely. We pay the price that we are now looking for rational points on a small subvariety of that described in the more direct approach above (and so may be missing out on rational points elsewhere), but gain the advantage that the resulting defining equations are vastly simplified. We usually (as will be the case with the genus 2 examples of Section 3) choose $\mathscr{R}$ so that $V(\mathscr{S}_m, \mathscr{R})$ is a curve; if all but one of the w_i's are linear in the induced equations, then the curve $V(\mathscr{S}_m, \mathscr{R})$ will be of genus 0, yielding a 1-parameter family of curves (the specialisation of $\mathscr{C}$) with an N-torsion divisor.

It was found that, for small N, it was better initially to run through many choices of $\mathscr{R}$, and to see whether an $\mathscr{R}$ existed which induced an obvious curve of genus 0, abandoning a given $\mathscr{R}$ once more than 2 of the w_i's became quadratic in the defining equations.

3. APPLICATIONS

We shall derive curves of genus 2 over $\mathbb{Q}$ with rational 11- and 13-torsion divisors, and of genus 4 over $\mathbb{Q}$ with a rational 29-torsion divisor.

For $N=11$, $g=2$, let $\mathscr{S}_m$ be as in Example 1.2, let $D_1 = \{(0, 0), \infty^+\}$, and let $\mathscr{R} = \{R_1, R_2\}$, where $R_1 : 2D_1 = \{(0, -w_1), (0, -w_1)\}$, $R_2 : 5D_1 = -6D_1$. The condition R_1 induces

$$w_5 = 2, \qquad w_4 = w_2 - w_1.$$

Given R_1, it is immediate that $2D_1, 3D_1, 4D_1$ may be obtained by degenerate additions to give

$$2D_1 = \{(0, -w_1), (0, -w_1)\}, \qquad 3D_1 = \{\infty^+, (0, -w_1)\},$$
$$4D_1 = \{\infty^+, \infty^+\}.$$

The system $\mathscr{S}_5(\mathscr{C}, \mathscr{O})$, together with this choice of $\mathscr{R}$, was given a high weighting by the searching program (which ran through many choices of $\mathscr{S}_m$ and $\mathscr{R}$), due to the linearity of the induced equations and the presence of the above degenerate additions in $\langle D_1 \rangle$.

We now perform the non-degenerate additions $D_1 + 4D_1$ and $-2D_1 - 4D_1$; comparing the resulting polynomials $a_{5D_1}(x)$ and $a_{-6D_1}(x)$, we find the equations induced by R_2,

$$w_2 = 2, \qquad w_3 = w_1 + 3,$$

taking care to avoid the 'false' solution $w_1 = 0$, for which $\mathscr{C}$ has genus < 2. Substituting these four equations into (1) gives the following family of genus 2 curves over $\mathbb{Q}$ in the parameter $t = w_1$.

APPLICATION 3.1. The family of curves of genus 2 ($t \neq 0$),

$$Y^2 + tY + (2-t)\,XY = X^2(X^4 + 2X^3 + (t+3)\,X^2 + 2X + t),$$

has the 11-torsion divisor D_1. In hyperelliptic form,

$$Y^2 = X^6 + 2X^5 + (2t+3)\,X^4 + 2X^3 + (t^2+1)\,X^2 + 2t(1-t)\,X + t^2$$

has the 11-torsion divisor $\{+\infty, (0, t)\}$.

To find 13-torsion over $\mathbb{Q}$ in dimension 2, we take the 5-parameter system of curves of genus 2 given by

$$\mathscr{C}: Y^2 - w_1 Y + w_2 XY = w_1 w_3 X^2(X-1)(X-w_4)(x-w_5) \qquad (2)$$

together with $\mathscr{O} = [2\infty]$ (again, the canonical divisor). Note that here ∞ is a $K(\mathbf{w})$-rational Weierstrass point. Let $D_1 = \{(0, 0), (1, 0)\}$ and take $\mathscr{R} = \{R_1, R_2\}$ where R_1, R_2 are the conditions $2D_1 = -\{(1, 0), \infty\}$, $6D_1 = -7D_1$, respectively.

Now, R_1 induces $w_4 = w_5 = 1$. Given R_1, all multiples of D_1 up to $6D_1$ may be obtained by degenerate additions to give $6D_1 = \{(0, 0), (0, 0)\}$. In a similar manner to 3.1, we find that the equations now induced by R_2 are $w_2 = 2w_1$ and $w_3 = -w_1$. Substituting these four equations in (2) gives the following family over $\mathbb{Q}$ in the parameter $t = w_1$.

APPLICATION 3.2. The family of curves of genus 2 ($t \neq 0$),

$$Y^2 - tY + 2tXY = -t^2X^2(X-1)^3,$$

has the 13-torson divisor $\{(0,0), (1,0)\}$.

If the genus of our system is allowed to increase, we find that there is a much greater flexibility in the choice of $\mathscr{R}$, and consequently a higher multiple of some D_1 which may be obtained by degenerate additions. It is reasonable, then, to expect the method to find further rational torsions as the genus is increased. We give the reader some idea of this greater flexibility in higher genus by deriving 29-torsion over $\mathbb{Q}$ in dimension 4.

We require $N=29$, $g=4$, and we use the $(10,4)$-system

$$\begin{aligned}\mathscr{C}: Y^2 + w_1 Y + w_2 XY + w_3 X^2 Y + w_4 X^3 Y + 2(2w_5 + w_6) X^4 Y \\ = X^{10} + 2w_6 X^9 + w_7 X^8 + w_8 X^7 + w_9 X^6 + w_{10} X^5 \end{aligned} \tag{3}$$

together with $\mathscr{O} = [2\infty^+ + 2\infty^-]$ (*not* the canonical divisor) where, as usual, ∞^+, ∞^- represent the branches of the singularity at infinity. Divisor classes in $\mathrm{Pic}^0_{K(w)}(\mathscr{C})$ are represented by sets of 4 points $\{P_1, P_2, P_3, P_4\}$ on $\mathscr{C}$. Three such sets sum to $\mathscr{O}$ if there is a function of the form (linear polynomial in X) $Y-$(sextic polynomial in X) which meets $\mathscr{C}$ at all 12 component points; this gives an explicit means of computing the (non-degenerate) group law in $\mathrm{Pic}^0_{K(w)}(\mathscr{C})$. Note that whereas in the genus 2 examples the representation of divisor classes by $\{P_1, P_2\}$ was unique away from $\mathscr{O}$, in this case we have the subtle ambiguity that two sets of the forms $\{(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_3, \tilde{y}_3)\}$ and $\{(x_1, y_1), (x_2, y_2), (x_4, y_4), (x_4, \tilde{y}_4)\}$ are equivalent (where $\tilde{y}_i = y_i - w_1 - w_2 x_i - w_3 x_i^2 - w_4 x_i^3 - 2(2w_5 + w_6) x_i^4$). In practice, such ambiguous representations (which correspond to a space of codimension 2) are computationally easy to deal with; in this case we replace any subset of the form $\{(x_i, y_i), (x_i, \tilde{y}_i)\}$ by the symbol $W^{(2)}$ (a 'Weierstrass Pair'), which will then count as two points in the set; for example, $\mathscr{O} = \{W^{(2)}, W^{(2)}\}$. We further take our intended rational 29-torsion to be $D_1 = \{\infty^+, (0,0), \infty^+, \infty^-\} = \{\infty^+, (0,0), W^{(2)}\}$.

Now take $\mathscr{R} = \{R_1, R_2\}$, where $R_1 : D_1 = -2\{(0,0), (0,0), (0,0), (0,0)\}$, $R_2 : 4D_1 = -\{\infty^+, \infty^+, \infty^+, (0,0)\}$. To see that $\mathscr{R}$ does indeed imply $ND_1 = \mathscr{O}$ (which is not as immediate as the previous examples), note that R_2 implies that $14D_1$ may be determined entirely by degenerate additions as $\{(0,0), (0,0), (0,0), (0,0)\}$. R_1 then becomes $D_1 = -28D_1$.

The condition R_1 is easily shown to be equivalent to the four equations $w_i = w_{11-i}$ $(i = 1 \cdots 4)$ by considering the function $Y - X^5$ (which then meets $\mathscr{C}$ with multiplicity 9 at $(0,0)$, 1 at ∞^+, and at $W^{(2)}$). Performing

the non-degenerate addition $2D_1+2D_1$ (by means of the function $(X+w_5+w_6)\,Y-X^5(X-w_5+w_6)$), we obtain four further equations induced by R_2, linear in all w_i's apart from w_5, w_6. Substituting these eight equations into (3), we obtain the following family over $\mathbb{Q}$ in the parameters $s=2w_5$, $t=w_5+w_6$.

APPLICATION 3.3. The 2-parameter family of genus 4 curves $(s, t\neq 0)$,

$$Y^2+st^4Y-st^3XY+st^2X^2Y-stX^3Y+(s+2t)\,X^4Y$$
$$=X^{10}+(2t-s)\,X^9-stX^8+st^2X^7-st^3X^6+st^4X^5,$$

has $D_1=\{\infty^+, (0,0), W^{(2)}\}$ as a 29-torsion divisor.

It is not immediately clear how increasing the genus affects the possible multiples of some D_1 which may be obtained entirely by degenerate additions. On the basis of some rather unsystematic experimentation with various choices of $\mathscr{S}_m$ and $\mathscr{R}$, it is the author's guess that all multiples up to an amount (at least) linear in g may be so obtained by suitable choices of $\mathscr{R}$; these should provide torsions over $\mathbb{Q}$ which also increase (at least) linearly with respect to g. Indeed, we hope that our method will give a constructive proof of the following conjecture.

Conjecture 3.4. There exists a constant κ, independent of g, such that for every $m\leqslant \kappa g$ there exists a hyperelliptic curve of genus g over $\mathbb{Q}$ with a rational m-torsion divisor.

Rational torsion divisors have relevance to the computer integration of algebraic functions (see [4]). By way of illustration we give an example (courtesy of James Davenport and his computer integration program) of an algebraic function whose integrability in terms of elementary functions corresponds to the rational 11-torsion found in 3.1, with $t=2$.

EXAMPLE 3.5. Consider

$$Y^2=X^6+2X^5+7X^4+3X^2+5X^2-4X+4.$$

Then, from the fact that $\{+\infty, (0,2)\}$ is an 11-torsion divisor, we may derive the function $(11X^2+6X+7)/Y$, whose integral can be expressed in terms of elementary functions. Explicitly,

$$\int (11X^2+6X+7)/Y\,dX=\mathrm{LOG}(\Phi_1(X)\,Y+\Phi_2(X)),$$

where

$$\Phi_1(X) = X^8 + 4X^7 + 16X^6 + 28X^5 + 49X^4 + 28X^3 + 24X^2 - 20X + 9$$

and

$$\Phi_2(X) = X^{11} + 5X^{10} + 23X^9 + 54X^8 + 117X^7 + 133X^6 + 155X^5 + 30X^4 + 49X^3 - 43X^2 + 63X - 14.$$

REFERENCES

1. J. BILLING AND K. MAHLER, On exceptional points on cubic curves, *J. London Math. Soc.* **15** (1940), 32–43.
2. D. G. CANTOR, Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.* **48** (1987), 95–101.
3. J. W. S. CASSELS, The Mordell–Weil group of curves of genus 2, *in* "Arithmetic and Geometry Papers Dedicated to I. R. Shafarevich on the Occasion of this Sixtieth Birthday. Vol. 1. Arithmetic," pp. 29–60, Birkhäuser, Boston, 1983.
4. J. H. DAVENPORT, "On the Integration of Algebraic Functions," Lecture Notes in Computer Science, Vol. 102, Springer-Verlag, Berlin/New York, 1981.
5. D. GRANT, Formal groups in genus 2, *J. Reine Angew. Math.*, to appear.
6. B. LEVI, Saggio per una teoria arithmetica delle forme cubiche ternaire, *Atti R. Accad.* **41** (1906), 739–764.
7. MAZUR, B. Rational points of modular curves, *in* "Modular Functions of One Variable, *V*," pp. 107–148, Lecture Notes in Mathematics, Vol. 601, Springer-Verlag, Berlin/New York, 1977.
8. M. A. REICHERT, Explicit determination of non-trivial torsion structures of elliptic curves over quadratic number fields, *Math. Comp.* **47** (1986), 637–658.
9. J. H. SILVERMAN, "The Arithmetic of Elliptic Curves," Springer-Verlag, Berlin/New York, 1986.