JOURNAL OF NUMBER THEORY **53**, 229-240 (1995)

Complete Systems of Two Addition Laws for Elliptic Curves

W. BOSMA*

Department of Pure Mathematics, University of Sydney, Sydney, New South Wales 2006, Australia

AND

H. W. LENSTRA, JR.[†]

Department of Mathematics, University of California, Berkeley, California 94720-3840

Received January 20, 1993; revised July 15, 1993

Let E be an elliptic curve over a field k, given in Weierstrass form. The addition law $E \times E \to E$ can be described by a finite number of triples of bihomogeneous polynomials, each triple being valid on an open subset of $E \times E$. In this paper we prove that the minimal number of triples that is needed equals two, and that this can only be achieved with polynomials of bidegree (2,2). Our approach leads to a specific set of two triples with the desired property. © 1995 Academic Press, Inc.

1. INTRODUCTION

Let k be a field, and let E be an elliptic curve over k, given by a Weierstrass equation $F(x, y, z) = 0$. The set $E(k)$ of points $(x:y:z)$ in the projective plane $\mathbf{P}^2(k)$ satisfying the equation forms in a natural way an abelian group, which is written additively, and which has $O = (0:1:0)$ as its zero element.

The usual algorithm for adding two points P_1, P_2 on E, which can be found in [5, Chapter III, Section 2], distinguishes five cases. Four special formulae cover the cases in which

$$P_1 = O, \text{ or } P_2 = O, \text{ or } P_1 = -P_2, \text{ or } P_1 = P_2.$$

* E-mail: wieb@maths.su.oz.au.

[†] E-mail: hwl@math.berkeley.edu.

A fifth formula covers the remaining case. Thus, the last formula is valid when (P_1, P_2) is in some *open* subset of $E \times E$, whereas the four special formulae are valid on certain *closed* subsets only. In the present paper we consider only formulae that are valid on open subsets of $E \times E$.

By an *addition law* on E we mean an addition formula for E that is valid on an open subset of $E \times E$; the precise definition is given in Section 2. Each addition law is a triple of polynomials in the coordinates $x_1, y_1, z_1, x_2, y_2, z_2$ of the points to be added, and each of these polynomials is *bihomogeneous*, that is, homogeneous in x_1, y_1, z_1 and homogeneous in x_2, y_2, z_2. A pair of points P_1, P_2 on E is called *exceptional* for an addition law if that addition law cannot be used to add P_1 and P_2. This occurs only if the three polynomials vanish simultaneously at the coordinates of the points P_1 and P_2.

By a *complete system of addition laws* on E we mean a collection of addition laws on E with the property that for any pair of points P_1, P_2 on E at least one of the addition laws in the collection can be used to add P_1 and P_2; in other words, no pair is exceptional for all the addition laws in the collection.

From the fact that the addition $E \times E \to E$ is a morphism of varieties (see [5, Chapter III, Theorem 3.6]) it follows that a complete system of addition laws on E exists. Indeed, a complete system of three addition laws, each consisting of bihomogeneous polynomials of bidegree $(2, 2)$, was exhibited explicitly by Lange and Ruppert [2; cf. 1]. In the present paper we show that there are complete systems consisting of *two* addition laws, and that both addition laws in such a system are necessarily of bidegree $(2, 2)$.

THEOREM 1. *The smallest cardinality of a complete system of addition laws on E equals two, and if two addition laws form a complete system then each of them has bidegree* $(2, 2)$.

We can describe all addition laws of bidegree $(2, 2)$. To do this, we omit the zero addition law, for which *all* pairs P_1, P_2 are exceptional, and we call two addition laws *equivalent* if there exists a non-zero element $d \in k$ such that the three polynomials in the first addition law are d times those in the second.

THEOREM 2. *There is a bijection between* $\mathbf{P}^2(k)$ *and the set of equivalence classes of non-zero addition laws of bidegree* $(2, 2)$ *on E that has the following property. If* $(a:b:c) \in \mathbf{P}^2(k)$ *and* P_1, P_2 *are points in* $E(K)$ *for some extension field K of k, then the pair* P_1, P_2 *is exceptional for the addition law corresponding to* $(a:b:c)$ *if and only if the difference* $P_1 - P_2$ *of* P_1 *and* P_2 *in the group* $E(K)$ *lies on the intersection of* $E(K)$ *and the line* $ax + by + cz = 0$ *in* $\mathbf{P}^2(K)$.

We see from this theorem that any two distinct lines in $\mathbf{P}^2(k)$ that intersect outside $E(k)$ give rise to a complete system of two addition laws on E. This occurs for instance for the lines $y=0$, $z=0$, and also for the lines $by+cz=0$, $b'y+c'z=0$ whenever $b, c, b', c' \in k$ are such that $bc'-b'c \neq 0$.

Theorem 2 implies the existence of a complete system of two addition laws, by the argument just given. The other assertions of Theorem 1 are proved in Section 3, and Theorem 2 is proved in Section 4. Section 5 contains explicit formulae, both for the bijection in Theorem 2 and for a complete system of two addition laws.

It will be seen that the coefficients of the Weierstrass equation for E enter polynomially into all formulae in Section 5. This implies that the same formulae can be used to perform the addition on elliptic curves over commutative *rings*. For rings with a trivial Picard group this is discussed in [3, Section 3]. In particular, it is shown in [3] how a complete system of addition laws leads to an efficient algorithm for adding two points on an elliptic curve over a finite ring. For this application to rings, it is essential that each of the addition formulae in the system is valid on an *open* subset of $E \times E$; thus, the traditional formulae as in [5, Chapter III, Section 2] cannot be used.

2. Addition Laws

Let the elliptic curve E be given by a Weierstrass equation

$$F(x, y, z)=0,$$
$$F(X, Y, Z)=Y^2Z+a_1XYZ+a_3YZ^2-X^3-a_2X^2Z-a_4XZ^2-a_6Z^3$$

with coefficients a_1, a_2, a_3, a_4, a_6 in k and with a non-zero discriminant (see [5, Chapter III, Section 1]). The set $E(k)$ of points of E over k forms in a natural way an abelian group, which is written additively, and which has $O=(0:1:0)$ as its zero element.

Let μ, ν be positive integers. By an *addition law of bidegree* (μ, ν) on E we mean a triple of polynomials $X_3, Y_3, Z_3 \in k[X_1, Y_1, Z_1, X_2, Y_2, Z_2]$ with the following properties. Firstly, they are bihomogeneous of bidegree (μ, ν), that is, homogeneous of degree μ in the variables X_1, Y_1, Z_1 and homogeneous of degree ν in the variables X_2, Y_2, Z_2. Secondly, whenever K is an extension field of k and $P_1=(x_1:y_1:z_1)$ and $P_2=(x_2:y_2:z_2)$ are in $E(K)$, then the elements $x_3=X_3(x_1, y_1, z_1, x_2, y_2, z_2)$, $y_3=Y_3(x_1, y_1, z_1, x_2, y_2, z_2)$, $z_3=Z_3(x_1, y_1, z_1, x_2, y_2, z_2)$ of K either satisfy $x_3=y_3=z_3=0$, or the point $P_3=(x_3:y_3:z_3) \in \mathbf{P}^2(K)$ is in $E(K)$ and equals the sum P_1+P_2 in the abelian group $E(K)$. We shall call a pair P_1, P_2 *exceptional* for the addition law if the first alternative holds.

A *complete system of addition laws* on E is a collection of addition laws with the property that for any pair $P_1, P_2 \in E(K)$ as above at least one of the addition laws in the collection can be used to add P_1 and P_2.

We denote by $k(E)$ the function field of E. It is the subfield of the field of fractions of $k[X, Y, Z]/(F)$ generated by k, X/Z, and Y/Z. Similarly, we write $k(E \times E)$ for the function field of $E \times E$, which is the subfield of the field of fractions of the ring

$$S = k[X_1, Y_1, Z_1, X_2, Y_2, Z_2]/(F(X_1, Y_1, Z_1), F(X_2, Y_2, Z_2))$$

generated by k, X_1/Z_1, Y_1/Z_1, X_2/Z_2, and Y_2/Z_2.

Let μ, ν be positive integers. Whether or not a triple X_3, Y_3, Z_3 of bihomogeneous polynomials of bidegree (μ, ν) forms an addition law on E clearly depends only on the images of X_3, Y_3, Z_3 in S. In the rest of this paper we shall accordingly view the polynomials constituting an addition law as elements of S. Since the map $k[X_1, Y_1, Z_1, X_2, Y_2, Z_2] \to S$ is injective when restricted to the piece of bidegree $(2, 2)$ this makes no difference for Theorem 2. Notice that the set of addition laws of bidegree (μ, ν) on E has a natural k-vector space structure.

Let $p_1, p_2, m\colon E \times E \to E$ denote the first projection, the second projection, and the addition map, respectively. We write

$$V = p_1^{-1} O, \qquad H = p_2^{-1} O, \qquad \nabla = m^{-1} O.$$

These are divisors on $E \times E$: the vertical divisor, the horizontal divisor, and the antidiagonal divisor.

Lemma. *Let μ, ν be positive integers. Then the map that sends an addition law X_3, Y_3, Z_3 to $Z_3 Z_1^{-\mu} Z_2^{-\nu}$ is a k-vector space isomorphism between the set of addition laws of bidegree (μ, ν) on E and the set of all $h \in k(E \times E)$ of which the divisor satisfies $(h) \geqslant 3 \cdot \nabla - 3\mu \cdot V - 3\nu \cdot H$.*

This lemma is essentially equivalent to a result that was derived by Lange and Ruppert (see [1, Section 2, first page]). Write L for the line bundle $\mathscr{L}(3 \cdot O)$ on E. This is a very ample line bundle on E, and the associated complete embedding of E into projective space is the given embedding $E \subset \mathbf{P}^2$. Lange and Ruppert argue that the set of addition laws of bidegree (μ, ν) on E is, as a k-vector space, isomorphic to the set of homomorphisms $m^*L \to p_1^* L^\mu \otimes p_2^* L^\nu$ of sheaves on $E \times E$, which in turn is isomorphic to the set of global sections of the line bundle $m^*L^{-1} \otimes p_1^* L^\mu \otimes p_2^* L^\nu$. This leads to the lemma, since

$$m^*L^{-1} \otimes p_1^* L^\mu \otimes p_2^* L^\nu = \mathscr{L}(-3 \cdot \nabla + 3\mu \cdot V + 3\nu \cdot H).$$

In explicit terms, the lemma can be understood as follows. First, the map sending r to $rZ_1^{-\mu}Z_2^{-\nu}$ is an isomorphism of the space $S_{\mu,\nu}$ of bihomogeneous elements of bidegree (μ, ν) of S with the space $\{h \in k(E \times E) : (h) \geqslant -3\mu \cdot V - 3\nu \cdot H\}$. To pass to addition laws, we write $f = m^*(X/Z)$ and $g = m^*(Y/Z)$ for the images of X/Z, $Y/Z \in k(E)$ under the map $m^*\colon k(E) \to k(E \times E)$ induced by m. The addition laws of bidegree (μ, ν) are then the same as triples of the form $X_3 = fr$, $Y_3 = gr$, $Z_3 = r$, where r is an element of $S_{\mu,\nu}$ for which fr and gr belong to $S_{\mu,\nu}$ as well; i.e., each of the divisors $(rZ_1^{-\mu}Z_2^{-\nu})$, $(frZ_1^{-\mu}Z_2^{-\nu})$, $(grZ_1^{-\mu}Z_2^{-\nu})$ is at least $-3\mu \cdot V - 3\nu \cdot H$. Since X/Z and Y/Z have pole divisors $2 \cdot O$ and $3 \cdot O$ on E, the pole divisors of f and g on $E \times E$ are $2 \cdot \nabla$ and $3 \cdot \nabla$, respectively. Hence an element $r \in S_{\mu,\nu}$ gives rise to an addition law if and only if $h = rZ_1^{-\mu}Z_2^{-\nu}$ satisfies $(h) \geqslant 3 \cdot \nabla - 3\mu \cdot V - 3\nu \cdot H$. This is the assertion of the lemma.

For computational purposes, we observe that to find f, g it suffices to know a single non-zero addition law X_3, Y_3, Z_3 on E, since $f = X_3/Z_3$, $g = Y_3/Z_3$. Such an addition law can be read from the usual algorithm for addition on $E(k)$: homogenizing the formula given in [5, Chapter III, 2.3], and removing a common factor Z_1Z_2, one obtains an addition law of bidegree $(2, 2)$. This is the first addition law given in Section 5.

3. Complete Systems of Minimal Cardinality

Let X_3, Y_3, Z_3 be a non-zero addition law of bidegree (μ, ν), and let $h = Z_3Z_1^{-\mu}Z_2^{-\nu}$. We put

$$D = (h) + 3\mu \cdot V + 3\nu \cdot H - 3 \cdot \nabla.$$

By the lemma, this is an effective divisor on $E \times E$, and it is linearly equivalent to $3\mu \cdot V + 3\nu \cdot H - 3 \cdot \nabla$. One readily verifies that a pair of points P_1, P_2 on E is exceptional for the addition law if and only if (P_1, P_2) is on the support of D. For this reason we call D the *exceptional divisor* associated to the addition law.

Any non-zero addition law has $\mu \geqslant 2$ and $\nu \geqslant 2$. To prove this, let D be the associated exceptional divisor, and for an integer n, let $\Gamma_n \subset E \times E$ be the graph of the map $E \to E$ sending P to nP. Since D is effective, the intersection product $D \cdot \Gamma_n$ is non-negative, at least for those n for which Γ_n is not a component of D. From

$$V \cdot \Gamma_n = 1, \qquad H \cdot \Gamma_n = n^2, \qquad \nabla \cdot \Gamma_n = (n+1)^2,$$

$$D \sim 3\mu \cdot V + 3\nu \cdot H - 3 \cdot \nabla$$

we thus see that

$$3(\mu+n^2\nu-(n+1)^2)\geqslant 0$$

for almost all integers n. Therefore $\nu\geqslant 2$. By symmetry, we have $\mu\geqslant 2$.

We turn to the proof of Theorem 1. If a single addition law would constitute a complete system, then it would have no exceptional pairs and the exceptional divisor would be zero. This contradicts that its bidegree $(3\mu-3, 3\nu-3)$ is different from $(0, 0)$.

Next suppose that two addition laws of bidegrees (μ, ν) and (κ, λ) constitute a complete system. We prove that $\mu=\nu=\kappa=\lambda=2$. Denote by D and C the associated exceptional divisors, so that

$$D\sim 3\mu\cdot V+3\nu\cdot H-3\cdot\nabla, \qquad C\sim 3\kappa\cdot V+3\lambda\cdot H-3\cdot\nabla.$$

No pair of points on E is exceptional for both addition laws. Therefore D and C have disjoint supports, and $D\cdot C=0$. From

$$V\cdot H=V\cdot\nabla=H\cdot\nabla=1, \qquad V\cdot V=H\cdot H=\nabla\cdot\nabla=0$$

we thus find that

$$9(\mu\lambda+\nu\kappa-\mu-\nu-\kappa-\lambda)=0,$$

which is the same as

$$(\mu-1)(\lambda-1)+(\nu-1)(\kappa-1)=2.$$

Since we know that $\mu, \lambda, \nu, \kappa\geqslant 2$ it follows that we have equality throughout, as asserted.

To finish the proof of Theorem 1 it will now suffice to show that there exists a complete system of two addition laws. As noted in the introduction, this is a consequence of Theorem 2, which is proved in the next section.

4. Addition Laws of Bidegree (2, 2)

In this section we prove Theorem 2. We retain the notation introduced earlier. In addition, we write $s\colon E\times E\to E$ for the subtraction map, and we let $\Delta=s^{-1}O$ be the diagonal divisor on $E\times E$.

Since the pole divisor of X/Z on E is $2\cdot O$, the pole divisor of $X_1/Z_1=p_1^*(X/Z)$ on $E\times E$ is $2\cdot p_1^{-1}O=2\cdot V$, and likewise the pole divisor of X_2/Z_2 is $2 \cdot H$. Hence the pole divisor of $h_0 = X_1/Z_1 - X_2/Z_2$ is $2 \cdot V + 2 \cdot H$. Also, h_0 clearly vanishes on Δ, and since a point P on E and its opposite $-P$ have the same x-coordinate it also vanishes on ∇. Therefore we have $(h_0) \geqslant \Delta + \nabla - 2 \cdot V - 2 \cdot H$. The difference is an effective divisor of bidegree $(0, 0)$ and is therefore zero. This proves that

$$(h_0) = \Delta + \nabla - 2 \cdot V - 2 \cdot H$$

(cf. [2, Lemma 1.3]; the existence of h_0 reflects a general property of symmetric invertible sheaves on abelian varieties, see [4, Section 3, Proposition 1]). We shall write

$$Z_0 = h_0^3 Z_1^2 Z_2^2 = (X_1 Z_2 - Z_1 X_2)^3/(Z_1 Z_2).$$

Applying the lemma from Section 2 with $\mu = \nu = 2$ and $h = h_0^3$ we find that there is an addition law X_3, Y_3, Z_3 of bidegree $(2, 2)$ on E for which Z_3 is equal to Z_0.

The map sending h to h/h_0^3 is an isomorphism from the set of those $h \in k(E \times E)$ with $(h) \geqslant 3 \cdot \nabla - 6 \cdot V - 6 \cdot H$ to the set of those $h \in k(E \times E)$ with $(h) \geqslant -3 \cdot \Delta$. Composing this with the isomorphism from the lemma we obtain an isomorphism

$$\{\text{addition laws of bidegree } (2, 2) \text{ on } E\} \rightarrow \{h \in k(E \times E) \colon (h) \geqslant -3 \cdot \Delta\}$$

that maps an addition law X_3, Y_3, Z_3 to $h = Z_3/Z_0$; the exceptional divisor associated to X_3, Y_3, Z_3 is then $(h) + 3 \cdot \Delta$. From $\Delta = s^{-1}O$ it follows that there is a map

$$s^* \colon \{h \in k(E) \colon (h) \geqslant -3 \cdot O\} \rightarrow \{h \in k(E \times E) \colon (h) \geqslant -3 \cdot \Delta\}.$$

As in [1, Section 2, third paragraph] one deduces from the fact that s has connected fibres that this map is an isomorphism as well. Since $\{h \in k(E) \colon (h) \geqslant -3 \cdot O\}$ is a three-dimensional k-vector space with basis X/Z, Y/Z, 1, one concludes that there is an isomorphism of k-vector spaces $k \times k \times k \rightarrow \{\text{addition laws of bidegree } (2, 2) \text{ on } E\}$ that sends (a, b, c) to the triple X_3, Y_3, Z_3 given by

$$Z_3 = (as^*(X/Z) + bs^*(Y/Z) + c)\, Z_0, \qquad X_3 = fZ_3, \qquad Y_3 = gZ_3.$$

Here $f = m^*(X/Z)$ and $g = m^*(Y/Z)$ are as in Section 2. The exceptional divisor of this addition law is the pullback, under s, of the divisor $((aX + bY + cZ)/Z) + 3 \cdot O$ on E. Its support is the inverse image under s of the intersection of E with the line $ax + by + cz = 0$. This proves Theorem 2.

5. Explicit Formulae

From [5, Chapter III, 2.3] it follows that $f = m^*(X/Z)$ and $g = m^*(Y/Z)$ are given by

$$f = \lambda^2 + a_1\lambda - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2, \qquad g = -(\lambda + a_1)f - \nu - a_3,$$

where

$$\lambda = \frac{Y_1Z_2 - Y_2Z_1}{X_1Z_2 - X_2Z_1} \quad \text{and} \quad \nu = -\frac{Y_1X_2 - Y_2X_1}{X_1Z_2 - X_2Z_1}.$$

Applying the automorphism of $E \times E$ mapping (P_1, P_2) to $(P_1, -P_2)$ we find that

$$s^*(X/Z) = \kappa^2 + a_1\kappa - \frac{X_1Z_2 + X_2Z_1}{Z_1Z_2} - a_2$$

and

$$s^*(Y/Z) = -(\kappa + a_1)\, s^*(X/Z) - \mu - a_3,$$

where

$$\kappa = \frac{Y_1Z_2 + Y_2Z_1 + a_1X_2Z_1 + a_3Z_1Z_2}{X_1Z_2 - X_2Z_1}$$

and

$$\mu = -\frac{Y_1X_2 + Y_2X_1 + a_1X_1X_2 + a_3X_1Z_2}{X_1Z_2 - X_2Z_1}.$$

The bijection of Theorem 2 maps $(0:0:1)$ to the addition law given by $X_3^{(1)} = fZ_0$, $Y_3^{(1)} = gZ_0$, $Z_3^{(1)} = Z_0$, which in explicit terms is found to be given by

$$\begin{aligned}
X_3^{(1)} = {} & (X_1Y_2 - X_2Y_1)(Y_1Z_2 + Y_2Z_1) + (X_1Z_2 - X_2Z_1)\, Y_1Y_2 \\
& + a_1X_1X_2(Y_1Z_2 - Y_2Z_1) + a_1(X_1Y_2 - X_2Y_1)(X_1Z_2 + X_2Z_1) \\
& - a_2X_1X_2(X_1Z_2 - X_2Z_1) + a_3(X_1Y_2 - X_2Y_1)\, Z_1Z_2 \\
& + a_3(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\
& - a_4(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& - 3a_6(X_1Z_2 - X_2Z_1)\, Z_1Z_2,
\end{aligned}$$

$$\begin{aligned}
Y_3^{(1)} = & -3X_1X_2(X_1Y_2 - X_2Y_1) \\
& - Y_1Y_2(Y_1Z_2 - Y_2Z_1) - 2a_1(X_1Z_2 - X_2Z_1)\,Y_1Y_2 \\
& + (a_1^2 + 3a_2)\,X_1X_2(Y_1Z_2 - Y_2Z_1) \\
& - (a_1^2 + a_2)(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\
& + (a_1a_2 - 3a_3)\,X_1X_2(X_1Z_2 - X_2Z_1) \\
& - (2a_1a_3 + a_4)(X_1Y_2 - X_2Y_1)\,Z_1Z_2 \\
& + a_4(X_1Z_2 + X_2Z_1)(Y_1Z_2 - Y_2Z_1) \\
& + (a_1a_4 - a_2a_3)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& + (a_3^2 + 3a_6)(Y_1Z_2 - Y_2Z_1)\,Z_1Z_2 \\
& + (3a_1a_6 - a_3a_4)(X_1Z_2 - X_2Z_1)\,Z_1Z_2, \\
Z_3^{(1)} = {} & 3X_1X_2(X_1Z_2 - X_2Z_1) - (Y_1Z_2 + Y_2Z_1)(Y_1Z_2 - Y_2Z_1) \\
& + a_1(X_1Y_2 - X_2Y_1)\,Z_1Z_2 - a_1(X_1Z_2 - X_2Z_1)(Y_1Z_2 + Y_2Z_1) \\
& + a_2(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) - a_3(Y_1Z_2 - Y_2Z_1)\,Z_1Z_2 \\
& + a_4(X_1Z_2 - X_2Z_1)\,Z_1Z_2.
\end{aligned}$$

The corresponding exceptional divisor is $3 \cdot \Delta$, so a pair of points P_1, P_2 on E is exceptional for this addition law if and only if $P_1 = P_2$.

Multiplying the addition law just given by $s^*(Y/Z)$ we obtain the addition law corresponding to $(0:1:0)$. It reads as follows:

$$\begin{aligned}
X_3^{(2)} = {} & Y_1Y_2(X_1Y_2 + X_2Y_1) + a_1(2X_1Y_2 + X_2Y_1)\,X_2Y_1 + a_1^2X_1X_2^2Y_1 \\
& - a_2X_1X_2(X_1Y_2 + X_2Y_1) - a_1a_2X_1^2X_2^2 + a_3X_2Y_1(Y_1Z_2 + 2Y_2Z_1) \\
& + a_1a_3X_1X_2(Y_1Z_2 - Y_2Z_1) - a_1a_3(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\
& - a_4X_1X_2(Y_1Z_2 + Y_2Z_1) - a_4(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) \\
& - a_1^2a_3X_1^2X_2Z_2 - a_1a_4X_1X_2(2X_1Z_2 + X_2Z_1) \\
& - a_2a_3X_1X_2^2Z_1 - a_3^2X_1Z_2(2Y_2Z_1 + Y_1Z_2) \\
& - 3a_6(X_1Y_2 + X_2Y_1)\,Z_1Z_2 \\
& - 3a_6(X_1Z_2 + X_2Z_1)(Y_1Z_2 + Y_2Z_1) - a_1a_3^2X_1Z_2(X_1Z_2 + 2X_2Z_1) \\
& - 3a_1a_6X_1Z_2(X_1Z_2 + 2X_2Z_1) + a_3a_4(X_1Z_2 - 2X_2Z_1)\,X_2Z_1 \\
& - (a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2)(Y_1Z_2 + Y_2Z_1)\,Z_1Z_2 \\
& - (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 + 4a_1a_2a_6 - a_1a_4^2)\,X_1Z_1Z_2^2 \\
& - a_3^3(X_1Z_2 + X_2Z_1)\,Z_1Z_2 - 3a_3a_6(X_1Z_2 + 2X_2Z_1)\,Z_1Z_2 \\
& - (a_1^2a_3a_6 - a_1a_3^2a_4 + a_2a_3^3 + 4a_2a_3a_6 - a_3a_4^2)\,Z_1^2Z_2^2,
\end{aligned}$$

$$\begin{aligned}
Y_3^{(2)} = {} & Y_1^2 Y_2^2 + a_1 X_2 Y_1^2 Y_2 + (a_1 a_2 - 3a_3)\, X_1 X_2^2 Y_1 \\
& + a_3 Y_1^2 Y_2 Z_2 - (a_2^2 - 3a_4)\, X_1^2 X_2^2 \\
& + (a_1 a_4 - a_2 a_3)(2X_1 Z_2 + X_2 Z_1)\, X_2 Y_1 \\
& + (a_1^2 a_4 - 2a_1 a_2 a_3 + 3a_3^2)\, X_1^2 X_2 Z_2 \\
& - (a_2 a_4 - 9a_6)\, X_1 X_2 (X_1 Z_2 + X_2 Z_1) \\
& + (3a_1 a_6 - a_3 a_4)(X_1 Z_2 + 2X_2 Z_1)\, Y_1 Z_2 \\
& + (3a_1^2 a_6 - 2a_1 a_3 a_4 + a_2 a_3^2 + 3a_2 a_6 - a_4^2)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) \\
& - (3a_2 a_6 - a_4^2)(X_1 Z_2 + X_2 Z_1)(X_1 Z_2 - X_2 Z_1) \\
& + (a_1^3 a_6 - a_1^2 a_3 a_4 + a_1 a_2 a_3^2 - a_1 a_4^2 + 4a_1 a_2 a_6 - a_3^3 - 3a_3 a_6)\, Y_1 Z_1 Z_2^2 \\
& + (a_1^4 a_6 - a_1^3 a_3 a_4 + 5a_1^2 a_2 a_6 + a_1^2 a_2 a_3^2 - a_1 a_2 a_3 a_4 - a_1 a_3^3 - 3a_1 a_3 a_6 \\
& - a_1^2 a_4^2 + a_2^2 a_3^2 - a_2 a_4^2 + 4a_2^2 a_6 - a_3^2 a_4 - 3a_4 a_6)\, X_1 Z_1 Z_2^2 \\
& + (a_1^2 a_2 a_6 - a_1 a_2 a_3 a_4 + 3a_1 a_3 a_6 + a_2^2 a_3^2 - a_2 a_4^2 \\
& + 4a_2^2 a_6 - 2a_3^2 a_4 - 3a_4 a_6)\, X_2 Z_1^2 Z_2 \\
& + (a_1^3 a_3 a_6 - a_1^2 a_3^2 a_4 + a_1^2 a_4 a_6 + a_1 a_2 a_3^3 \\
& + 4a_1 a_2 a_3 a_6 - 2a_1 a_3 a_4^2 + a_2 a_3^2 a_4 \\
& + 4a_2 a_4 a_6 - a_3^4 - 6a_3^2 a_6 - a_4^3 - 9a_6^2)\, Z_1^2 Z_2^2, \\
Z_3^{(2)} = {} & 3X_1 X_2 (X_1 Y_2 + X_2 Y_1) + Y_1 Y_2 (Y_1 Z_2 + Y_2 Z_1) + 3a_1 X_1^2 X_2^2 \\
& + a_1 (2X_1 Y_2 + Y_1 X_2)\, Y_1 Z_2 + a_1^2 X_1 Z_2 (2X_2 Y_1 + X_1 Y_2) \\
& + a_2 X_1 X_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + a_2 (X_1 Y_2 + X_2 Y_1)(X_1 Z_2 + X_2 Z_1) \\
& + a_1^3 X_1^2 X_2 Z_2 + a_1 a_2 X_1 X_2 (2X_1 Z_2 + X_2 Z_1) \\
& + 3a_3 X_1 X_2^2 Z_1 + a_3 Y_1 Z_2 (Y_1 Z_2 + 2Y_2 Z_1) \\
& + 2a_1 a_3 X_1 Z_2 (Y_1 Z_2 + Y_2 Z_1) \\
& + 2a_1 a_3 X_2 Y_1 Z_1 Z_2 + a_4 (X_1 Y_2 + X_2 Y_1)\, Z_1 Z_2 \\
& + a_4 (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1) \\
& + (a_1^2 a_3 + a_1 a_4)\, X_1 Z_2 (X_1 Z_2 + 2X_2 Z_1) + a_2 a_3 X_2 Z_1 (2X_1 Z_2 + X_2 Z_1) \\
& + a_3^2 Y_1 Z_1 Z_2^2 + (a_3^2 + 3a_6)(Y_1 Z_2 + Y_2 Z_1)\, Z_1 Z_2 \\
& + a_1 a_3^2 (2X_1 Z_2 + X_2 Z_1)\, Z_1 Z_2 + 3a_1 a_6 X_1 Z_1 Z_2^2 \\
& + a_3 a_4 (X_1 Z_2 + 2X_2 Z_1)\, Z_1 Z_2 + (a_3^3 + 3a_3 a_6)\, Z_1^2 Z_2^2.
\end{aligned}$$

A pair of points P_1, P_2 on E is exceptional for this addition law if and only if the y-coordinate of $P_1 - P_2$ is zero. The addition laws $X_3^{(1)}$, $Y_3^{(1)}$, $Z_3^{(1)}$ and $X_3^{(2)}$, $Y_3^{(2)}$, $Z_3^{(2)}$ form a complete system of addition laws on E.

Multiplying the first addition law by $s^*(X/Z)$ we obtain the addition law corresponding to $(1:0:0)$. It is given by

$$\begin{aligned}
X_3^{(3)} = {} & (X_1Y_2 + X_2Y_1)(X_1Y_2 - X_2Y_1) + a_1X_1X_2(X_1Y_2 - X_2Y_1) \\
& - a_3X_1X_2(Y_1Z_2 - Y_2Z_1) + a_3(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\
& + (a_1a_3 + a_4)\,X_1X_2(X_1Z_2 - X_2Z_1) \\
& + (a_3^2 + 3a_6)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& + (a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2)(X_1Z_2 - X_2Z_1)\,Z_1Z_2, \\
Y_3^{(3)} = {} & (X_1Y_2 - X_2Y_1)\,Y_1Y_2 + a_2X_1X_2(X_1Y_2 - X_2Y_1) \\
& + 2a_3(X_1Z_2 - X_2Z_1)\,Y_1Y_2 \\
& - (a_1a_3 + 3a_4)\,X_1X_2(Y_1Z_2 - Y_2Z_1) \\
& + (a_1a_3 + a_4)(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\
& - (a_1a_4 - a_2a_3)\,X_1X_2(X_1Z_2 - X_2Z_1) \\
& + (2a_3^2 + 3a_6)(X_1Y_2 - X_2Y_1)\,Z_1Z_2 \\
& - 3a_6(X_1Z_2 + X_2Z_1)(Y_1Z_2 - Y_2Z_1) \\
& - (3a_1a_6 - a_3a_4)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& - (a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2)(Y_1Z_2 - Y_2Z_1)\,Z_1Z_2 \\
& - (a_1^3a_6 - a_1^2a_3a_4 + a_1a_2a_3^2 + 4a_1a_2a_6 \\
& - a_1a_4^2 - a_3^3 - 3a_3a_6)(X_1Z_2 - X_2Z_1)\,Z_1Z_2, \\
Z_3^{(3)} = {} & -(X_1Y_2 + X_2Y_1)(Y_1Z_2 - Y_2Z_1) - (X_1Z_2 - X_2Z_1)\,Y_1Y_2 \\
& - a_1X_1X_2(Y_1Z_2 - Y_2Z_1) - a_1(X_1Y_2 + X_2Y_1)(X_1Z_2 - X_2Z_1) \\
& - (a_1^2 + a_2)\,X_1X_2(X_1Z_2 - X_2Z_1) - a_3(X_1Y_2 - X_2Y_1)\,Z_1Z_2 \\
& - a_3(X_1Z_2 + X_2Z_1)(Y_1Z_2 - Y_2Z_1) \\
& - (a_1a_3 + a_4)(X_1Z_2 + X_2Z_1)(X_1Z_2 - X_2Z_1) \\
& - (a_3^2 + 3a_6)(X_1Z_2 - X_2Z_1)\,Z_1Z_2.
\end{aligned}$$

A pair of points P_1, P_2 on E is exceptional for this addition law if and only if the x-coordinate of $P_1 - P_2$ is zero. This occurs if $P_1 = P_2$, so $X_3^{(1)}$, $Y_3^{(1)}$, $Z_3^{(1)}$ and $X_3^{(3)}$, $Y_3^{(3)}$, $Z_3^{(3)}$ do not form a complete system of addition laws on E. The addition laws $X_3^{(2)}$, $Y_3^{(2)}$, $Z_3^{(2)}$ and $X_3^{(3)}$, $Y_3^{(3)}$, $Z_3^{(3)}$

form a complete system if and only if the point with $x = y = 0$ does not lie on the curve, i.e., if and only if $a_6 \neq 0$.

The bijection of Theorem 2 sends $(a:b:c)$ to the sum of a times the third addition law, b times the second addition law, and c times the first one. For example, the three addition laws given in [2]—with b_4 in the top line of [2, p. 111] corrected to a_4—correspond to $(0:0:-1)$, $(1:0:0)$, and $(a_1:2:a_3)$, respectively.

Acknowledgments

The authors wish to thank Enrico Bombieri, Olivier Debarre, Carel Faber, and Hans-Georg Rück for helpful discussions. The first author was supported by the Australian Research Council (Grants A68830699 and A68930041). The second author was supported by NSF under Grant DMS 90-02939. Use was made of the computer algebra systems Cayley and Maple.

References

1. H. Lange and W. Ruppert, Complete systems of addition laws on abelian varieties, *Invent. Math.* **79** (1985), 603–610.
2. H. Lange and W. Ruppert, Addition laws on elliptic curves in arbitrary characteristics, *J. Algebra* **107** (1987), 106–116.
3. H. W. Lenstra, Jr., Elliptic curves and number-theoretic algorithms, *in* "Proceedings of the International Congress of Mathematicians, Berkeley, California, August 3–11, 1986" (A. M. Gleason, Ed.), American Mathematical Society, Providence, 1987.
4. D. Mumford, On the equations defining abelian varieties. I, *Invent. Math.* **1** (1966), 287–354.
5. J. H. Silverman, "The Arithmetic of Elliptic Curves," Springer-Verlag, New York, 1986.