ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 22, Number 1, Winter 1992

A GENERALIZATION OF A RESULT OF HURWITZ AND MORDELL ON THE TORSION SUBGROUPS OF CERTAIN ELLIPTIC CURVES

CHRIS CALDWELL

1. Introduction. Let k be an algebraic number field. For any elements a, b, c, d of k with $abc(d^3 - 27abc) \neq 0$, define an irreducible nonsingular cubic curve (over the field of complex numbers) by

$$F : aX^3 + bY^3 + cZ^3 = dXYZ.$$

Whenever the set of k-rational points $F(k)$ (points P in the projective plane with $P = (x, y, z)$ for some integers x, y, z of k) is not empty, F is an elliptic curve over k and $F(k)$ is an abelian group. We consider the problem of finding the torsion subgroup of $F(k)$. We also give an infinite family of elliptic curves over the rational numbers $\mathbf{Q}$ with rank at least two.

The rank of these curves has been very well studied, see [**1, 2, 3, 6, 12, 13, 14, 16**]. Yet previously the only general result about the torsion subgroup of $F(k)$, denoted here by $\mathrm{tor}\,(F(k))$, were the theorems of Hurwitz [**8**] and Mordell [**10,11**]. These authors did not use the modern language of elliptic curves, but their results may be written as follows

Theorem 1.1. (Hurwitz-Mordell) *Let a, b and c be squarefree nonzero rational integers, relatively prime in pairs. Let d be an integer such that $d^3 \neq 27abc$. Suppose that $F(\mathbf{Q})$ is not empty, and make F an elliptic curve over k by choosing any element of $F(\mathbf{Q})$ as the origin of F.*

(i) *If at most one of a, b, c is ± 1, then the only torsion point is the origin and the rank of $F(\mathbf{Q})$ is positive.*

(ii) *If $a = b = 1$, $c \neq \pm 1$, then $F(\mathbf{Q})$ has one or three torsion points. $F(\mathbf{Q})$ has three torsion points if and only if $d = c \pm 2$ or $4c \pm 1$.*

(iii) *If $a = b = c = 1$ and $d \neq -1, 5$, then $F(\mathbf{Q})$ has three torsion points.*

Received by the editors on October 15, 1988.

(iv) *If $a = b = c = 1$ and $d = -1, 5$, then $F(\mathbf{Q})$ has six torsion points.*

The result (iv) is due to Mordell, the others are due to Hurwitz.

Hurwitz's proof uses a function H mapping $F(\mathbf{Q})$ to the rational integers defined as follows. For each rational point P on F, choose relatively prime integers X, Y and Z with X nonnegative, such that $P = (X, Y, Z)$. Set $H(P) = XYZ$. Hurwitz showed that for every P in $F(\mathbf{Q})$, either $H(P) = 0$, or $H(P)$ divides $H(-2P)$. This divisibility property was the basis of his proof.

We generalize Hurwitz's function by defining a function $h_{k,F}$ from $F(k)$ into the ideals of k as follows. Let $[x_1, \ldots, x_n]$ denote the ideal of k generated by the integers $x_1, \ldots, x_n$ of k. For each point P in $F(k)$ choose integers X, Y, Z of k such that $P = (X, Y, Z)$, and define

$$h_{k,F}((X, Y, Z)) = \frac{[abc][XYZ]^3}{[aX^3, bY^3, cZ^3]^3}.$$

In section two we show $h_{k,F}$ is a well-defined function with divisibility properties similar to those of Hurwitz's function H.

In section three we show how to find the torsion points in $F(\mathbf{Q})$ whose orders are a power of two. In section four we turn our attention to the entire torsion group and generalize theorem 1.1 as follows.

Theorem 1.2. *Let k be a field which does not have a unit u such that $1 - u$ is also a unit. Let a, b, c and d be integers of k such that $[a], [b], [c]$ are square free ideals, and $d^3 \neq 27abc$. If none of $ab^{-1}, bc^{-1}, ac^{-1}$ are cubes in k, then $F(k)$ has no torsion. If ab^{-1} is a cube, then the number of points with odd order is one, if bc^{-1} is not a cube in k, and three otherwise. The number of points of order exactly two is one plus the number of zeros in k of*

$$abc\mathbf{X}^3 - d\mathbf{X} + 2.$$

We then find the following family of elliptic curves with rank at least two, and explain how to construct further examples.

Corollary 1.3. *Let m and n be odd relatively prime rational integers such that $a = n(n^2 - 2m^2)$ is prime to seven and squarefree. Define an elliptic curve C with origin 0_C as follows,*

$$C : aX^3 + aY^3 + 7Z^3 = -7m^2XYZ, \qquad 0_C = (1, -1, 0).$$

Then $(1, -1, m)$ and $(1, -2, n)$ generate a subgroup of $C(\mathbf{Q})$ with rank two.

We conclude this section by recalling the addition formulae for the curve F. These formulae were first formulated by Cauchy [**4**] and greatly simplified by Desbones [**5**].

Let T_3 be the set of nine inflection points of F. Letting ρ be a primitive cube root of unity, these points are

$$\begin{array}{lll} (-b^{1/3}, a^{1/3}, 0), & (-c^{1/3}, 0, a^{1/3}), & (0, -c^{1/3}, b^{1/3}) \\ (-b^{1/3}, a^{1/3}\rho, 0), & (-c^{1/3}, 0, a^{1/3}\rho), & (0, -c^{1/3}, b^{1/3}\rho) \\ (-b^{1/3}, a^{1/3}\rho^2, 0), & (-c^{1/3}, 0, a^{1/3}\rho^2), & (0, -c^{1/3}, b^{1/3}\rho^2). \end{array} \tag{1}$$

For these points, we find

$$\begin{aligned} (x, y, z) + (-b^{1/3}, a^{1/3}\rho^j, 0) &= (\rho^j x, \rho^{2j} y, z) \\ (x, y, z) + (-c^{1/3}, 0, a^{1/3}\rho^j) &= (b^{2/3}c^{1/3}\rho^{2j} y, a^{1/3}c^{2/3}\rho^j z, a^{2/3}b^{1/3}x) \\ (x, y, z) + (0, -c^{1/3}, b^{1/3}\rho^j) &= (b^{1/3}c^{2/3}\rho^j z, a^{2/3}c^{1/3}\rho^{2j} x, a^{1/3}b^{2/3}y). \end{aligned} \tag{2}$$

Let $P_i = (x_i, y_i, z_i)$ $(i = 1, 2, 3)$ and $P_3 = -P_1 - P_2$. If at most one of P_1, P_2 is in T_3, then

$$x_3 = x_1^2 y_2 z_2 - x_2^2 y_1 z_1, \quad y_3 = y_1^2 x_2 z_2 - y_2^2 x_1 z_1, \quad z_3 = z_1^2 x_2 y_2 - z_2^2 x_1 y_1. \tag{3}$$

The formula for multiplying by -2 on the curve F is

$$-2(x, y, z) = (x(by^3 - cz^3), \quad y(cz^3 - ax^3), \quad z(ax^3 - by^3)). \tag{4}$$

If $(b^{1/3}, -a^{1/3}, 0)$ is the origin of F, then

$$-(x, y, z) = (b^{2/3}y, a^{2/3}x, (ab)^{1/3}z). \tag{5}$$

Finally, notice that the set of inflection points T_3 may alternately be characterized by each of the following:

(i) T_3 is the set of points (x, y, z) on F for which $xyz = 0$.

(ii) T_3 is the set of points P on F for which $P = -2P$.

(iii) If $(b^{1/3}, -a^{1/3}, 0)$ is the origin of F, then T_3 is the set of points whose orders divide three.

2. A height function. Let k be any number field containing the coefficients of our curve F. Define a function $h_{k,F}$ mapping the k-rational points of F into the ideals of k by

$$h_{k,F}(P) = \frac{[abc][xyz]^3}{[ax^3, by^3, cz^3]^3} \tag{6}$$

where x, y, z are any integers of k such that $P = (x, y, z)$. The key properties of $h_{k,F}$ are listed in the following theorem.

Theorem 2.1. *Let $h_{k,F}$ be as above. Then, for all points P, P' in $F(k)$*

(i) *$h_{k,F}(P)$ is a well-defined integral ideal.*

(ii) *$h_{k,F}(P) = [0]$ if and only if P is an element of $T_3(k)$.*

(iii) *$GCD(h_{k,F}(P), h_{k,F}(P'))$ divides $h_{k,F}(-P - P')$.*

When $(a/b)^{1/3}$ is an element of k and the origin of F is chosen to be $(b^{1/3}, -a^{1/3}, 0)$, then we have

(iv) *$h_{k,F}(P) = h_{k,F}(-P)$.*

(v) *Let m be an integer, $h_{k,F}(P)$ divides $h_{k,F}(mP)$.*

(vi) *Let P have order n. If m is an integer prime to n, then $h_{k,F}(P) = h_{k,F}(mP)$.*

(vii) *$h_{k,F}(P + Q) = h_{k,F}(P)$ for all points Q in $T_3(k)$.*

Proof. If L is any finite extension of the rationals containing the field k and R is the ring of integers of L, then for all points P in $F(k)$ we have

$$h_{L,F}(P) = h_{k,F}(P) \cdot R, \qquad h_{k,F}(P) = h_{L,F}(P) \cap k.$$

The statements in this theorem involve only the divisibility or equality of ideals, so it is sufficient to prove the theorem for $L = k(\rho, a^{1/3}, b^{1/3}, c^{1/3})$. Hence, we assume k contains $a^{1/3}, b^{1/3}, c^{1/3}$ and ρ.

Define a new curve B, and a birational map π mapping F to B as follows. Let $D = (abc)^{-1/3}d$,

$$B : X^3 + Y^3 + Z^3 = DXYZ \qquad \pi(x, y, z) = (a^{1/3}x, b^{1/3}y, c^{1/3}z).$$

Let $\wp$ be a fixed prime ideal of k. For integers x_i of k, let $\operatorname{ord}(x_1, \ldots, x_n)$ be the order at $\wp$ of the ideal generated by $x_1, \ldots, x_n$. Notice that if $\pi(x, y, z) = (X, Y, Z)$ with x, y, z, X, Y, Z in k, then

$$\begin{aligned} 3(\operatorname{ord}(XYZ) - \operatorname{ord}(X^3, Y^3, Z^3)) \\ = \operatorname{ord}(abc) + 3\operatorname{ord}(xyz) - 3\operatorname{ord}(ax^3, by^3, cz^3). \end{aligned}$$

That is, $\operatorname{ord}(h_{k,B}(X, Y, Z)) = \operatorname{ord}(h_{k,F}(x, y, z))$. This is true for all prime ideals $\wp$ of k, so the two heights are equal. Thus, it is sufficient to prove the theorem for the curve function $h_{k,B}$.

The function $h_{k,B}$ is a perfect cube, so we prove this theorem for the function on B given by the cube root of $h_{k,B}$:

$$h((x, y, z)) = \frac{[xyz]}{[x, y, z]^3}.$$

Claim (i) of the theorem is now obvious. Claim (ii) is true because T_3 is the set of points (x, y, z) with $xyz = 0$. Claims (iv) and (vii) are clear by the addition formulas (5) and (2), respectively.

We next show that claims (v) and (vi) follow from claim (iii). Assume (iii) holds for h. This implies $h(P)$ divides $h(-P - P) = h(\pm 2P)$ (by (iv)). So again by claim (iii), $h(P)$ divides $h(-P - 2P) = h(\pm 3P)$. We can continue this process and prove claim (v) by induction. To see (vi) let P have order n and let m be a rational integer prime to n. There exists a rational integer m' for which the product $m'm$ is congruent to one modulo n, so by claim (v) we know $h(P)$ divides $h(mP)$ and also $h(mP)$ divides $h(m'mP) = h(P)$. This proves claim (vi).

To complete the proof, we must show h satisfies claim (iii). Equivalently, we must show that if $-P_1 - P_2 = P_3$ for points P_i of $B(k)$, then for each prime $\wp$ of k

$$\min\{\operatorname{ord}(h(P_1)),\ \operatorname{ord}(h(P_2))\} \leq \operatorname{ord}(h(P_3)). \tag{7}$$

The proof of this relation is purely computational and is left until section five.

Example 2.2. The curve $C : 4x^3 + 2y^3 + z^3 = -3xyz$ has exactly three points defined over $\mathbf{Q}$:

$$(1,-1,1), \qquad (1,-1,-2), \qquad (1,2,-2).$$

At each of these points $h_{\mathbf{Q},C}$ is equal to $[\mathbf{8}]$. Let β b any cube root of two and choose $0_C = (-1,\beta,0)$ as the origin of C. The curve C has nine points defined over $k = \mathbf{Q}(\beta)$:

$$\begin{array}{lll} P = (1,-1,1) & 2P = (-1,\beta^2,-2\beta) & 3P = (0,-1,\beta) \\ 4P = (1,2,-2) & 5P = (\beta,1,-\beta^2) & 6P = (-1,0,\beta^2) \\ 7P = (1,-1,2) & 8P = (-1,\beta^2,\beta) & 9P = (-1,\beta,0) = 0_C. \end{array}$$

$h_{\mathbf{Q}(\beta),C}$ takes on the value $[\mathbf{8}]$ at $P, 2P, 4P, 5P, 7P$ and $8P$; and the value $[0]$ at $3P, 6P$ and $9P$.

Remark 2.3. It is possible to make the functions $h_{k,F}$ independent of the field k by setting

$$h_F(x,y,z) = [\mathrm{Norm}_{\mathbf{L}/\mathbf{Q}}(h_{\mathbf{L},F}(x,y,z))]^{1/[\mathbf{L}:\mathbf{Q}]}$$

where $\mathbf{L}$ is any number field containing k over which (x,y,z) is defined. This is well defined but not necessarily an integer. We do not use h_F in this work because the divisibility properties for which $h_{k,F}$ was defined are much less apparent.

3. Points with order a power of two. Define an elliptic curve A over k by

$$A : X^3 + Y^3 + abcZ^3 = dXYZ.$$

Sylvester [**15**] defined a rational map $\mu : F(k) \to A(k)$ by

$$\mu : (x,y,z) \longrightarrow (X,Y,Z)$$

where

$$\begin{aligned} X &= ab^2x^3y^6 + bc^2y^3z^6 + a^2cz^3x^6 - 3abcx^3y^3z^3 \\ Y &= a^2bx^6y^3 + b^2cy^6z^3 + ac^2z^6x^3 - 3abcx^3y^3z^3 \\ dZ &= a^3x^9 + b^3y^9 + c^3z^9 - 3abcx^3y^3z^3. \end{aligned}$$

A rational map between abelian varieties is a homomorphism plus a translation. Thus, μ will be a homomorphism if we choose $\mu\ (0_F)$ to be the origin of A. μ has degree nine so the kernel of μ is the points of order three. Thus, to determine the subgroup of torsion points with orders prime to three in $F(k)$, it is sufficient to find in $A(k)$ the (isomorphic) subgroup of torsion points with orders prime to three.

Every choice of origin for $A(k)$ yields an isomorphic group structure, so we choose $(-1,1,0)$ as the origin of $A(k)$. Let $P=(x,y,z)$ be a point on A with order two. Recall xyz is zero if and only if (x,y,z) is a point with order three; thus, $xyz\neq 0$ and we may assume $x=1$. Now $-2(1,y,z)=(-1,1,0)$ with (4) yields

$$y(cz^3-1)=h, \qquad y^3-cz^3=-h, \qquad z(1-y^3)=0$$

for some constant of proportionality h in k. These equalities show that $y=1$. Solving for z in the equation defining A, we find

Lemma 3.1. *Let $0_A=(-1,1,0)$ be the origin of A. The points of A with order dividing two are the origin 0_A, and the three points $(1,1,Z_i)$ where Z_1,Z_2,Z_3 are the zeros of*

$$abcZ^3-dZ+2=0. \tag{8}$$

If F is an elliptic curve over k, then the number of points with order two in $F(k)$ is one plus the number of zeros in k of (8).

The integer two is prime in the Euclidean domain $\mathbf{Q}(\rho)$, allowing us to easily find the following.

Example 3.2. Suppose that $k=\mathbf{Q}(\rho)$, a,b,c,d are integers of k, and abc is squarefree. F has a point of order two if and only if

$$abc=\rho^i d\pm 2, \quad \text{or} \quad 4abc=\rho^i d\pm 1$$

with $i=0,1$ or 2. The points are $(-1,-1,\pm\rho^i)$, $(-1,-1,\pm 2\rho^i)$, respectively.

We conclude this section with a result which gives us a way to find all the points of order 2^i on A (hence on F).

Lemma 3.3. *Let $P = (r, s, t)$ be a point on A. If $rst = 0$, then $-2P = P$. If $rst \neq 0$, then the points Q for which $-2Q = P$ are given by $Q = (1, Y, Z)$ where Y and Z satisfy the following equations:*

$$tY + Z(rY + s) = 0 \tag{9}$$

$$rY^4 + 2sY^3 + tdY^2 + 2rY + s = 0. \tag{10}$$

Proof. If $rst = 0$, then P is in the set T_3 and, therefore, $-2P = P$. So assume $rst \neq 0$. Let $P = -2(X, Y, Z)$ for some complex numbers X, Y, Z. By the addition formula (4) (and $r \neq 0$) we know $X \neq 0$. So we may further assume $X = 1$. Again, using the addition formula (4) we have

$$Y^3 - cZ^3 = rw, \qquad Y(cZ^3 - 1) = sw, \qquad Z(1 - Y^3) = tw$$

for some constant of proportionality w of k. Eliminating w we find

$$(rY + s)cZ^3 = (sY^2 + r)Y, \qquad -tcZ^3 = rZ(1 - Y^3) - tY^3.$$

Combining to eliminate cZ^3, we find

$$r(1 - Y^3)[Z(rY + s) + tY] = 0. \tag{11}$$

If $1 - Y^3 = 0$, then $t = 0$. $rst \neq 0$, so in this case (11) is just (9). We now find (10) by using (9) and (11) to eliminate Z from the equation for A.

4. The torsion subgroup. To simplify the statements of our next results, we will call a nonsingular cubic F *admissible* if $[a]$, $[b]$ and $[c]$ are squarefree integral ideals of k and d is an integer of k.

Theorem 4.1. *Let F be admissible and let $P = (x, y, z)$ be a point of $F(k)$. $h_{F,k}(P)$ divides $h_{F,k}(-2P)$. If $h_{F,k}(P) = h_{F,k}(-2P)$, then either P is in T_3, $-2P$ is in T_3, or there exists a unit u of k such that $1 - u$ is a unit and $-2(x, y, z) = (x, -uy, (u - 1)z)$.*

Section six is entirely devoted to the very computational proof of this theorem. In this section we explore the theorem's consequences beginning with our generalization of the Hurwitz-Mordell result.

Corollary 4.2. *Let F be admissible. Suppose that k does not have a unit u such that $1-u$ is also a unit. If none of $ab^{-1}, bc^{-1}, ac^{-1}$ are cubes in k, then $F(k)$ has no torsion. If ab^{-1} is a cube, then the number of torsion points with odd order is one when bc^{-1} is not a cube in k and three otherwise.*

Proof. If $ab^{-1}, ab^{-1}, ac^{-1}$ are not cubes, then the intersection of T_3 and $F(k)$ is empty. Thus, for every point P in $F(k)$, we know by Theorem 4.1 that $h_{k,F}(P)$ properly divides $h_{F,k}(-2P)$, which properly divides $h_{k,F}(4P)$, which properly divides $h_{k,F}(-8P)$, etc. So P cannot be a torsion point. On the other hand, if ab^{-1} is a cube, let $0_F = (b^{1/3}, -a^{1/3}, 0)$. If P is a torsion point with odd order, then by Theorem 2.1 $h_{k,F}(P) = h_{k,F}((-2)^i P)$, so by Theorem 4.1 P is an element of T_3. Looking at (1) we see the number of points in T_3 which are k-rational is one if bc^{-1} is not a cube and three if bc^{-1} is a cube.

We now find an infinite family of elliptic curves with ranks at least two.

Corollary 4.3. *Let m and n be odd relatively prime rational integers such that $a = n(n^2 - 2m^2)$ is prime to seven and squarefree. Define an elliptic curve C over $\mathbf{Q}$ as follows*

$$C : aX^3 + aY^3 + 7Z^3 = -7m^2XYZ, \qquad 0_C = (1, -1, 0).$$

The points $(1, -1, m)$ and $(1, -2, n)$ generate a subgroup of $C(\mathbf{Q})$ with rank two.

Proof. By Corollary 4.2, $C(\mathbf{Q})$ has no two torsion so the points $P_1 = (1, -1, m)$ and $P_2 = (1, -2, n)$ of C are points of infinite order (thus rank $(C(\mathbf{Q})) > 0$). Assume, for contradiction, rank $(C(\mathbf{Q})) = 1$. Let $P = (x, y, z)$ be a generator with x, y, z relatively prime integers. Because a is squarefree we may assume further that x, y, z are pairwise relatively prime, hence $h_{\mathbf{Q},C}(P) = [7a][xyz]^3/[a, z]^3$. By Theorem 2.1 (parts v and vii) $h_{\mathbf{Q},C}(P)$ divides $GCD(h_{\mathbf{Q},C}(P_1), h_{\mathbf{Q},C}(P_2)) = [7a]$,

i.e., $[xyz]$ divides $[a, z]$ and it follows that $xy = \pm 1$. The only points satisfying this are 0_C, P_1 and $-P_1$, so $P = \pm P_1$. This is a contradiction because $h_{\mathbf{Q},C}(P_1)$ divides $h_{\mathbf{Q},C}(P_2)$. □

Remark 4.4. In this construction of an infinite family of curves with rank two (or greater) it is not necessary to use the points $(1, -1, m)$, $(1, -2, n)$; we could have picked most any integers r, s, t, u and chosen C so that $C(\mathbf{Q})$ contains the points (r, s, m) and (t, u, n). Thus, we could easily construct infinitely many families of curves with ranks greater than one.

5. The completion of the proof of Theorem 2.1. In section two we began our proof of theorem 2.1 by proving claims (i), (ii), (iv) and (vii). We then showed claims (iv) and (v) follow easily from claim (iii), which in turn follows from the following inequality (7) for points $P_3 = -P_1 - P_2$ on the curve B.

$$\min\{\operatorname{ord}(h(P_1), \operatorname{ord}(h(P_2))\} \leq \operatorname{ord}(h(P_3)).$$

($\operatorname{ord}(l)$ is the order of the ideal l at a fixed prime ideal $\wp$ of k.) We now complete the proof by showing this inequality always holds.

If $h(P_1)h(P_2) = [0]$ (the zero ideal), then at least one of P_1, P_2 is a point of order three and we are done by claim (vii) of this theorem. Assume $h(P_1)h(P_2) \neq [0]$. The inequality (7) also clearly holds if $\operatorname{ord}(h(P_1))\operatorname{ord}(h(P_2)) = 0$, so we assume

$$0 < \operatorname{ord}(h(P_1)) \leq \operatorname{ord}(h(P_2)). \tag{12}$$

Choose x_i, y_i, z_i in k so that $P_i = (x_i, y_i, z_i)$, $i = 1, 2$. The curve B is homogeneous and there exists an element of the algebraic number field k with order one at $\wp$, so we may assume $\operatorname{ord}(x_i), \operatorname{ord}(y_i), \operatorname{ord}(z_i)$, $i = 1, 2$, are nonnegative and at least one of these three orders is zero for each point P_i, $i = 1, 2$.

Adding a point of the set T_3 to P_i rearranges the coordinates of P_i (by addition formula (1)), but does not alter the value of h (by claim (vii) of Theorem 2.1). Thus, we also assume

(13)

$$0 = \operatorname{ord}(z_1) \leq \operatorname{ord}(y_1) \leq \operatorname{ord}(x_1), \quad 0 = \operatorname{ord}(z_2) \leq \operatorname{ord}(x_2) \leq \operatorname{ord}(y_2).$$

From the definition of the map h, we have

$$\text{(14)}\quad \begin{aligned}&\operatorname{ord}(h(x,y,z))\\ &\quad = \operatorname{ord}(x)+\operatorname{ord}(y)+\operatorname{ord}(z)-3\min\{\operatorname{ord}(x),\operatorname{ord}(y),\operatorname{ord}(z)\}\end{aligned}$$

so, with our assumptions,

$$\text{(15)}\qquad \operatorname{ord}(h(P_1)) = \operatorname{ord}(x_1) + \operatorname{ord}(y_1), \qquad i = 1, 2.$$

Using (7), (12) and (15) we see that to prove the theorem it is sufficient to show the following

$$\text{(16)}\quad \begin{aligned}&\operatorname{ord}(x_1) + \operatorname{ord}(y_1)\\ &\quad \le \operatorname{ord}(x_3)+\operatorname{ord}(y_3)+\operatorname{ord}(z_3)-3\min\{\operatorname{ord}(x_3),\operatorname{ord}(y_3),\operatorname{ord}(z_3)\}.\end{aligned}$$

The remainder of this proof is divided into six cases:

(I) $P_1 \neq P_2$, $\operatorname{ord}(y_1) = \operatorname{ord}(x_2) = 0$

(II) $P_1 \neq P_2$, $\operatorname{ord}(y_1) = 0$, $\operatorname{ord}(x_2) > 0$

(III) $P_1 \neq P_2$, $\operatorname{ord}(y_1) > 0$, $\operatorname{ord}(x_2) = 0$

(IV) $P_1 \neq P_2$, $\operatorname{ord}(y_1), \operatorname{ord}(x_2) > 0$

(V) $P_1 = P_2$, $\operatorname{ord}(x_1) > 0$, $\operatorname{ord}(y_1) = \operatorname{ord}(z_2) = 0$

(VI) $P_1 = P_2$, $\operatorname{ord}(x_1, \operatorname{ord}(y_1 > 0$, $\operatorname{ord}(x_2) = 0$.

To begin cases (I) through (IV) we use the addition formula (1) to define elements x_3, y_3, z_3 of k so that $P_3 = (x_3, y_3, z_3)$.

(17)
$$x_3 = x_1y_2^2z_1 - x_2y_1^2z_2, \quad y_3 = x_2^2y_1z_1 - x_1^2y_2z_2, \quad z_3 = x_1y_1z_2^2 - x_2y_2z_1^2.$$

Case (I). $\operatorname{ord}(y_1) = \operatorname{ord}(x_2) = 0$, so by (12), (13), (15) and (17) we see $\operatorname{ord}(x_3) = \operatorname{ord}(y_3) = 0$. Thus, $\operatorname{ord}(x_1) \le \operatorname{ord}(z_3) = \operatorname{ord}(h(P_3))$ so $\operatorname{ord}(z_3) = 0$ (by (17), (12) and (14)). This shows the inequality (16) holds in case (I).

In cases (II), (III) and (IV), $\operatorname{ord}(D) < 0$. To see this, note that in each of these cases at least two of $\operatorname{ord}(x_i), \operatorname{ord}(y_i), \operatorname{ord}(z_i)$ are nonzero for either $i = 1$ or $i = 2$. If $\operatorname{ord}(D)$ is nonnegative, then all of $\operatorname{ord}(x_i), \operatorname{ord}(y_i), \operatorname{ord}(z_i)$ must be positive (by the equation of the curve)

which contradicts our assumption that at least one is zero. So for the proofs of (II), (III) and (IV) we assume $-\mathrm{ord}\,(D) = M > 0$.

Case (II). $\mathrm{ord}\,(x_2) > 0$, so $\mathrm{ord}\,(x_2^3 + y_2^3 + z_2^3) = \mathrm{ord}\,(z_2^3) = \mathrm{ord}\,(Dx_2y_2z_2) = 0$. This shows $\mathrm{ord}\,(x_2) + \mathrm{ord}\,(y_2) = M$. Also, $\mathrm{ord}\,(y_1) = 0$, so $0 \leq \mathrm{ord}\,(x_1^3 + y_1^3 + z_1^3) = \mathrm{ord}\,(Dx_1y_1z_1)$. This shows $M \leq \mathrm{ord}\,(x_1)$. Using these in (17), we find $\mathrm{ord}\,(x_3) = \mathrm{ord}\,(x_2)$, $\mathrm{ord}\,(y_3) = 2\mathrm{ord}\,(x-2)$, $M \leq \mathrm{ord}\,(z_3)$, from which the inequality (16) follows.

Case (III). If $\mathrm{ord}\,(x_2) = 0$ and $\mathrm{ord}\,(y_1) > 0$, then, by the same argument as in (II), we find

$$\mathrm{ord}\,(x_3) = 2\mathrm{ord}\,(y_1), \qquad \mathrm{ord}\,(y_3) = \mathrm{ord}\,(y_1), \qquad M \leq \mathrm{ord}\,(z_3),$$

and again the inequality (16) is clear.

Case (IV). If $\mathrm{ord}\,(y_1)\mathrm{ord}\,(x_2) \neq 0$, then we interchange x_2 and y_2 (by adding an element of T_3 which does not affect the heights by claim (vii)). As in (II), we know $\mathrm{ord}\,(x_1) + \mathrm{ord}\,(y_1) = \mathrm{ord}\,(y_2) + \mathrm{ord}\,(z_2) = M$. If all four orders are equal, then the result is trivial. Because $\mathrm{ord}\,(h(P_1)) = \mathrm{ord}\,(h(P_2))$, we may assume $\mathrm{ord}\,(y_2) > \mathrm{ord}\,(x_1)$ (by interchanging P_1, P_2 if necessary). Thus we now have

$$0 < \mathrm{ord}\,(z_2) < \mathrm{ord}\,(y_1) \leq \mathrm{ord}\,(x_1) < \mathrm{ord}\,(y_2).$$

Using this, we find

$$\mathrm{ord}\,(x_3) = 2\mathrm{ord}\,(y_1) + \mathrm{ord}\,(z_2),\ \mathrm{ord}\,(y_3) = \mathrm{ord}\,(y_1),\ \mathrm{ord}\,(z_3) = \mathrm{ord}\,(y_2)$$

and again the inequality (16) follows easily.

Finally, we treat the two cases with $P_1 = P_2 = (x, y, z)$. We may assume $0 = \mathrm{ord}\,(z) \leq \mathrm{ord}\,(y) \leq \mathrm{ord}\,(x)$ and $\mathrm{ord}\,(x) > 0$. Using the addition formula (4), we define x_3, y_3, z_3 by

$$x_3 = x(y^3 - z^3) \qquad y_3 = y(z^3 - x^3) \qquad z_3 = z(x^3 - y^3).$$

Case (V). If $\mathrm{ord}\,(y) = 0$, then $\mathrm{ord}\,(y_3) = \mathrm{ord}\,(z_3) = 0$, and $\mathrm{ord}\,(x_3) = \mathrm{ord}\,(x)$, showing the inequality (16) holds.

Case (VI). $\mathrm{ord}\,(y) > 0$, so we find

$$\mathrm{ord}\,(x) = \mathrm{ord}\,(x_3), \qquad \mathrm{ord}\,(y) = \mathrm{ord}\,(y_3), \qquad \mathrm{ord}\,(z)) \leq 3\mathrm{ord}\,(y_3),$$

from which the inequality (16) is clear. This completes the proof of Theorem 2.1.

6. The proof of Theorem 4.1. This section is devoted to the proof of Theorem 4.1. Let $P = (x, y, z)$ with x, y, z integers of k. If T_3 contains P or $-2P$, then the result of the theorem is obvious, so we assume T_3 contains neither of $P, -2P$. Recall the formula for multiplication by -2 on F is

$$-2(x, y, z) = (x(by^3 - cz^3), \quad y(cz^3 - ax^3), \quad z(ax^3 - by^3)).$$

Let $[x_1, x_2, \ldots, x_n]$ denote the ideal generated by the elements x_i of k, and for any ideals I and J of k, let $I + J$ denote the greatest common denominator of I and J. Define ideals $I_1, I_2, I_3, J_1, J_2, J_3$ of k by:

$$I_1 = [cz^3 - by^3], \qquad I_2 = [ax^3 - cz^3], \qquad I_3 = [ax^3 - by^3]$$
$$J_1 = [ax^3], \qquad J_2 = [by^3], \qquad J_3 = [cz^3].$$

These ideals are nonzero by part (ii) of Theorem 2.1. Using the definition (6) of $h_{k,F}$ and our hypothesis that $h_{k,F}(P) = h_{k,F}(-2P)$, we see

$$I_1 I_2 I_3 (J_1 + J_2 + J_3) = (J_1 I_1^3 + J_2 I_2^3 + J_3 I_3^3). \tag{18}$$

By adding the generators of I_2, I_3, we see

$$I_1 \mid I_2 + I_3. \tag{19}$$

(That is, I_1 divides $I_2 + I_3$.)

Lemma 6.1. *If J_i, $i = 1, 2, 3$, are defined as above, then*

$$J_1 \mid J_2 + J_3, \qquad J_2 \mid J_1 + J_3, \qquad J_3 \mid J_1 + J_2. \tag{20}$$

The proof uses the special form of F and is delayed until the end of this section.

Define new ideals I, J, I'_i, J'_i, $i = 1,2,3$ by $I = I_1 + I_2 + I_3$, $J = J_1 + J_2 + J_3$, $I_i = I'_i I$ and $J_i = J'_i J$, $i = 1,2,3$. Now (18), (19) and (20) become

$$I'_1 I'_2 I'_3 = J'_1 I'^3_1 + J'_2 I'^3_2 + J'_3 I'^3_3 \tag{21}$$

$$[1] = I'_1 + I'_2 = I'_1 + I'_3 \tag{22}$$

$$[1] = J'_2 + J'_3 = J'_1 + J'_3 = J'_1 + J'_2. \tag{23}$$

In particular, (21) shows that I'_i divides $J'_2 I'^3_2 + J'_3 I'^3_3$, so (22) implies I'_1 divides $J'_1 + J'_2$; and finally, (23) implies I'_1 is [1]. Thus, by symmetry,

$$[1] = I'_i = I'_2 = I'_3 \quad \therefore \quad I_1 = I_2 = I_3.$$

This shows that there exist units u_1 and u_2 of k for which

$$cz^3 - by^3 = u_1^{-1}(cz^3 - ax^3) = u_2^{-1}(ax^3 - by^3). \tag{24}$$

Eliminating x,

$$(u_1 + u_2 - 1)(cz^3 - by^3) = 0.$$

Assume for contradiction that $u_1 + u_2 \neq 0$, then $cz^3 = by^3$ and $3ax^3 = 3by^3 = 3cz^3 = dabc$. Thus, $(x,y,z) = (a^{-1/3}, b^{-1/3}, c^{-1/3})$, $d^3 = 27abc$, and F has genus zero. This is a contradiction because F is nonsingular, hence $u_1 + u_2 = 1$. Finally, (4) and (24) imply $-2(x,y,z) = (-x, u_1 y, u_2 z)$, completing the proof of this theorem. □

Proof of Lemma 6.1. We assume for proof by contradiction that $J_2 + J_3$ does not divide J_1. So there is at least one prime $\wp$ of k such that

$$\min\{\operatorname{ord}(J_2), \quad \operatorname{ord}(J_3)\} > \operatorname{ord}(J_1) \tag{25}$$

where $\operatorname{ord}(I)$ denotes the order of the ideal I of k at the prime $\wp$.

By (25) and the equation defining the curve F, we know $\operatorname{ord}(J_1) = \operatorname{ord}([dxyz])$. This may be written

$$\operatorname{ord}(a) - \operatorname{ord}(d) = (\operatorname{ord}(y) - \operatorname{ord}(x)) + (\operatorname{ord}(z) - \operatorname{ord}(x)). \tag{26}$$

Notice the left side of this equality is less than $\operatorname{ord}(a)$, which (because F is admissible) is at most one.

Using the definitions of J_i, $i = 1, 2, 3$, the restrictions on the ideals $[a], [b]$, and (25), we see

$$\begin{aligned} 2 &> \operatorname{ord}(b) - \operatorname{ord}(a) > 3[\operatorname{ord}(x) - \operatorname{ord}(y)] \\ 2 &> \operatorname{ord}(c) - \operatorname{ord}(a) > 3[\operatorname{ord}(x) - \operatorname{ord}(z)]. \end{aligned} \tag{27}$$

This shows that $\operatorname{ord}(x) \leq \operatorname{ord}(y)$ and $\operatorname{ord}(x) \leq \operatorname{ord}(z)$. By (26) at least one of these must be an equality, say $\operatorname{ord}(x) = \operatorname{ord}(y)$, then, by (27), $\operatorname{ord}(b) = 1$ and $\operatorname{ord}(a) = 0$. Finally, $\operatorname{ord}(a) = 0$ in (26) implies $\operatorname{ord}(x) = \operatorname{ord}(y) = \operatorname{ord}(z)$, and $\operatorname{ord}(c) = \operatorname{ord}(b) = 1$.

Using the definition (6) of the function h we see that

$$\operatorname{ord}(h_{k,F}(x, y, z)) = 2 \quad \text{and} \quad \operatorname{ord}(h_{k,F}(-2(x, y, z))) > 4,$$

giving the desired contradiction. □

REFERENCES

1. S. Akhtar, *Elliptic curves with points of order three*, Punjab Univ. J. Math. **8** (1975), 41–50.

2. E.T. Avanesov, *On the equation* $Ax^3 + By^3 + Cz^3 = Nxyz$, (Russian) Dokl. BSSR Akad. Nauk. **23** (1978).

3. C. Caldwell, *The elliptic curve* $aX^3 + bY^3 + cZ^3 = dXYZ$, Thesis, University of California (Berkeley), 1984.

4. A.L. Cauchy, *Exercices de Mathematiques*, Paris, 1827, 233–270.

5. M. Desbones, *Resolution, En Nombres Entires Et Sous Sa Forme Plus General, De L'equation Cubique, Homogene, a Trois Inconnues*, Nouv. Ann. de Math. Ser. III **5**, 1886.

6. Eric Dofs, *On some classes of homogeneous ternary cubic Diophantine equations*, Ark. Mat. **13** (1957), 29–72.

7. B.A. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Math. **776**, Springer-Verlag, New York, 1980.

8. A. Hurwitz, *Ueber ternare diophantische Gleichungen dritte Grades*, Viertel Jahrschrift Naturf. Ges. Zurich, 1917, 207–229.

9. S. Lang, *Elliptic curves: diophantine analysis* (Grundlehren der mathematischen Wissenschaften) **231**, Springer-Verlag, Berlin, 1978.

10. L.J. Mordell, *The diophantine equation* $X^3 + Y^3 + Z^3 + kXYZ = 0$, Colloque sur la theorie des nombres, Bruxelles, 1955, 67–76.

11. ———, *Diophantine equations*, Academic Press, Boston, 1969.

12. P. Satge, *Une generalization du calcul de Selmer*, Seminar on Number Theory, Paris, 1981–82. Progr. Math. **38**, Birkhauser, Boston, (1983), 245–265.

13. E.S. Selmer, *The diophantine equation* $aX^3 + bY^3 + cZ^3 = 0$, Acta Math. **85** (1951), 203–362.

14. ———, *The diophantine equation* $aX^3 + bY^3 + cZ^3 = 0$. Completion of the Tables, Acta Math. **92** (1954), 191–197.

15. J.J. Sylvester, Collected Works (1909), vol **1**, 118 (contains many misprints).

16. E. Thomas and A. Vasque, *Diophantine equations arising from cubic number fields*, J. Number Theory **13** (1981)m, 398–414.

Department of Mathematics & Computer Science, University of Tennessee at Martin, Martin, TN 38238