ACTA ARITHMETICA
LXXIX.1 (1997)

Some special curves of genus 5

by

Andrew Bremner (Tempe, Ariz.)

Dedicated to Professor J. W. S. Cassels on the occasion of his 75th birthday

1. Let $Q_i(l,m)$, $i = 1,2,3$, be three non-proportional non-singular diagonal quadratic forms with rational coefficients:

$$Q_i(l,m) \equiv a_i l^2 + b_i m^2, \tag{1}$$

and denote by E the curve of intersection

$$Q_1(l,m) = r^2, \quad Q_2(l,m) = s^2, \quad Q_3(l,m) = t^2. \tag{2}$$

Then E is an irreducible curve in $\mathbb{P}^4$ of degree 8 and genus 5. Suppose there exists a point on (2) whose coordinates generate an extension field of $\mathbb{Q}$ of odd degree n. It is straightforward to see by Riemann–Roch that E possesses an effective rational divisor of degree 5, henceforth referred to as a *rational pentuple* on E. Such a pentuple may not be irreducible over $\mathbb{Q}$, for instance comprising a rational pair and a rational triple.

We are concerned with how to determine whether or not the curve E can possess rational pentuples. No such pentuple, and E can have no points defined over extension fields of $\mathbb{Q}$ of odd degree.

The approach is modelled directly on that of Cassels [2]; see also Bremner [1]. The Jacobian of the curve E is of dimension 5, and is in fact isogenous to the product of five elliptic curves. It suffices to produce natural maps from E to each of five curves E_i of genus 1, for then there are induced morphisms from $\mathrm{Jac}(E)$ to $\mathrm{Jac}(E_i)$, and the latter is isomorphic to an elliptic curve. The five morphisms then induce the required isogeny.

1991 *Mathematics Subject Classification*: 11D25, 11G05, 11G10, 11G30, 11G35, 14G25.

We can display five curves E_i of genus 1, with respective maps $\mu_i : E \to E_i$ given by projection:

$$\begin{aligned}
E_1: &\quad a_1l^2 + b_1m^2 = r^2, \\
&\quad a_2l^2 + b_2m^2 = s^2, \\
&\qquad \mu_1(l,m,r,s,t) = (l,m,r,s); \\
E_2: &\quad a_1l^2 + b_1m^2 = r^2, \\
&\quad a_3l^2 + b_3m^2 = t^2, \\
&\qquad \mu_2(l,m,r,s,t) = (l,m,r,t); \\
E_3: &\quad a_2l^2 + b_2m^2 = s^2, \\
&\quad a_3l^2 + b_3m^2 = t^2, \\
&\qquad \mu_3(l,m,r,s,t) = (l,m,s,t); \\
E_4: &\quad a_2r^2 + (a_1b_2 - a_2b_1)m^2 = a_1s^2, \\
&\quad a_3r^2 + (a_1b_3 - a_3b_1)m^2 = a_1t^2, \\
&\qquad \mu_4(l,m,r,s,t) = (m,r,s,t); \\
E_5: &\quad b_2r^2 - (a_1b_2 - a_2b_1)l^2 = b_1s^2, \\
&\quad b_3r^2 - (a_1b_3 - a_3b_1)l^2 = b_1t^2, \\
&\qquad \mu_5(l,m,r,s,t) = (l,r,s,t).
\end{aligned}$$

Denote by G_i the group $E_i(\mathbb{Q})$ of rational points on E_i, $i = 1, \ldots, 5$. Certainly a rational pentuple on E projects onto a rational pentuple of points on each E_i, and again by Riemann–Roch, each E_i contains an effective divisor of degree 1, that is, there exists a rational point on E_i. Consequently, if any G_i is empty, there cannot exist a rational pentuple on E.

Henceforth we assume that each G_i is non-empty; and by choosing a rational point O_i in G_i as the zero-point, each E_i may be given the structure of Abelian variety of dimension 1 over $\mathbb{Q}$. By abuse of notation, this Abelian variety will also be denoted by E_i.

We now give an explicit method for determining rational points on each E_i from a rational pentuple on E. Corresponding to the map μ_j, denote by μ_{j*} the "push-forward" map from the group of divisors on E to the group of divisors on E_j (see, for example, Fulton [4]). For a rational pentuple T on E_j define $\nu_j(T)$ to be the unique point on E_j satisfying the linear equivalence

$$\nu_j(T) \sim \mu_{j*}(T) - \Pi_j \tag{3}$$

where Π_j is a hyperplane section of E_j. A specific construction for $\nu_j(T)$ is easily given. Cut E_j by a quadric through $\mu_{j*}(T)$; then the plane through the three residual points of this intersection cuts E_j residually in $\nu_j(T)$.

2. Given a rational pentuple T on E, we show below how to construct a rational pentuple S on E such that the points $\nu_i(S)$ in G_i, $i = 1, \ldots, 5$, are restricted to a finite set. It then remains (see Section 3) to determine from such finite sets of rational points on $E_1, \ldots, E_5$ whether indeed they can arise from an *ur*-pentuple on E.

LEMMA 1. *Let T be a rational pentuple on E, and let $P \in G_1$. Then there is a rational pentuple S on E such that*

$$\nu_1(S) = \nu_1(T) - 2P, \tag{4}$$

$$\nu_j(S) = \nu_j(T), \quad j = 2,3,4,5. \tag{5}$$

Here, the subtraction in (4) *is that of G_1.*

Proof. Let μ_1^* be the "pull-back" map of divisors on E_1 to divisors on E, corresponding to the map μ_1. By Riemann–Roch, there is an effective rational divisor S on E satisfying the linear equivalence

$$S \sim T - \mu_1^*(P) + \mu_1^*(O_1). \tag{6}$$

Then

$$\begin{aligned}\nu_1(S) &\sim \mu_{1*}(S) - \Pi_1 \sim \mu_{1*}(T) - \Pi_1 - \mu_{1*}\mu_1^*(P) + \mu_{1*}\mu_1^*(O_1)\\ &\sim \nu_1(T) - 2P + 2O_1\end{aligned}$$

using (3) and the fact that $\mu_{1*}\mu_1^*$ is multiplication by the degree of μ_1 (see Fulton [4], Example 1.7.4). Via the Jacobian mapping, (4) now follows. Further, from (3) and (6), for $j = 2, \ldots, 5$,

$$\nu_j(S) \sim \mu_{j*}(S) - \Pi_j \sim \nu_j(T) - \mu_{j*}\mu_1^*(P) + \mu_{j*}\mu_1^*(O_1). \tag{7}$$

For clarity, consider $j = 2$. Suppose P is the point (l_p, m_p, r_p, s_p), and put $t_p^2 = Q_3(l_p, m_p)$. Then the points $\mu_{2*}\mu_1^*(P)$ on E_2 are the pair $(l_p, m_p, r_p, \pm t_p)$. From E_2 there is a natural restriction ϕ to the quadric Q_1 at (2) given by $\phi(l,m,r,t) = (l,m,r)$ and then $\mu_{2*}\mu_1^*(P) = \phi^{-1}(l_p, m_p, r_p)$. Similarly, denoting O_1 by (l_1, m_1, r_1, s_1), we have $\mu_{2*}\mu_1^*(O_1) = \phi^{-1}(l_1, m_1, r_1)$. However, any two points of a quadric are linearly equivalent, and so $(l_1, m_1, r_1) \sim (l_p, m_p, r_p)$ on Q_1. It follows that $\mu_{2*}\mu_1^*(P) \sim \mu_{2*}\mu_1^*(O_1)$ on E_2. More generally, $\mu_{j*}\mu_1^*(P) \sim \mu_{j*}\mu_1^*(O_1)$ on E_j for $j = 2,3,4,5$, so that (7) implies $\nu_j(S) \sim \nu_j(T)$ on E_j, and (5) follows. ∎

The referee observes that this proof is less mysterious if viewed in the following light.

Consider the commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\mu_1} & E_1 \\ {\scriptstyle \mu_2}\downarrow & & \downarrow{\scriptstyle \phi_1} \\ E_2 & \xrightarrow[\phi_2]{} & C_{12} \end{array}$$

where μ_1 and ϕ_2 "forget" t, and μ_2 and ϕ_1 "forget" s (with C_{12} the first quadric at (2)). Then E is the fibre product of E_1 and E_2, and it follows that $\mu_{2*}\mu_1^* = \phi_2^*\phi_{1*}$ (see Fulton [4], Prop. 1.7). Since $\phi_{1*}(P) \sim \phi_{1*}(O_1)$ on C_{12}, (5) follows as before. In this way, the lemma is seen as a special case

of a much more general result, and the proof extends entirely naturally to all combinations of i, j instead of 1, 2.

A geometric construction to produce such a pentuple S is as follows. The linear space of quadrics in $\mathbb{P}^4$ with basis $\{l^2, lm, lr, ls, lt, m^2, mr, ms, mt, rs, rt, st\}$ has 11 degrees of freedom. Cut E by a quadric of the system through T, $\mu_1^*(P)$, $2\mu_1^*(O_1)$. The intersection comprises 16 points, so the residual intersection is a rational pentuple R, say. Again cut E by a quadric through R, $2\mu_1^*(P)$, $\mu_1^*(O_1)$, having residual intersection a rational pentuple S. Then we have the following linear equivalence of divisors on E:

$$T + \mu_1^*(P) + 2\mu_1^*(O_1) + R \sim R + 2\mu_1^*(P) + \mu_1^*(O_1) + S,$$

so that $S \sim T - \mu_1^*(P) + \mu_1^*(O_1)$ as required.

Analogous lemmas to the above are obtained by replacing G_1 by G_i, $i = 2, 3, 4, 5$. There is the following consequence.

THEOREM 2. *For $j = 1, \ldots, 5$, let C_j denote a set of points on E_j forming a complete set of coset representatives for $G_j/2G_j$. Let T be a rational pentuple on E. Then there is a rational pentuple S on E such that $\nu_j(S) \in C_j$, $j = 1, \ldots, 5$.* ∎

3. We describe how to determine possible pentuples T from a knowledge of the $\nu_j(T)$. For this purpose, it is expedient to define an alternative map ν_j' from rational pentuples on E to rational points on E_j by defining $\nu_j'(T) \sim 2\Pi_j - 2O_j - \mu_{j*}(T)$. Then $\nu_j(T) + \nu_j'(T) \sim \Pi_j - 2O_j$ and it follows (N.B. the remark preceding Lemma 3) that $\nu_j'(T) \equiv \nu_j(T) \bmod 2G_j$. Accordingly, as before, $\nu_j'(T)$ can be restricted to a set C_j of representatives for $G_j/2G_j$.

Restrict attention to E_1, denoting O_1 by (l_1, m_1, r_1, s_1). The hyperplanes

$$l_1a_1l + m_1b_1m - r_1r = 0 = l_1a_2l + m_1b_2m - s_1s$$

each contain $2O_1$ in their intersection with E_1. Then given a rational pentuple T on E, there exist $a, b, c, d, e, f \in \mathbb{Q}$ such that the quadric

$$\begin{aligned}(8)\qquad \pi(l, m, r, s) \equiv (al + bm + cr + ds)(l_1a_1l + m_1b_1m - r_1r) \\ + (el + fm)(l_1a_2l + m_1b_2m - s_1s) = 0\end{aligned}$$

contains both $\mu_{1*}(T)$ and $2O_1$ in its intersection with E_1. The residual point of the intersection is $\nu_1'(T)$. Eliminating r, s between (8) and the equations for E_1 results in an equation $P_8(l, m) = 0$, where P_8 is homogeneous of degree 8, with coefficients which are homogeneous quartic polynomials in a, b, c, d, e, f. Perforce, P_8 factorizes in the form

$$(9)\qquad P_8(l, m) = (m_1l - l_1m)^2(\beta l - \alpha m)P_5(l, m)$$

where $\nu_1'(T) = (\alpha, \beta, \gamma, \delta)$, and $P_5(l, m)$ is homogeneous of degree 5, with roots for $l : m$ comprising the ratios $l : m$ for the five points of $\mu_{1*}(T)$ (so P_5 is irreducible over $\mathbb{Q}$ if and only if T is irreducible over $\mathbb{Q}$).

Write

$$P_8(l,m)/(m_1 l - l_1 m)^2 = (\beta l - \alpha m)P_5(l,m) \tag{10}$$
$$= c_0 l^6 + c_1 l^5 m + c_2 l^4 m^2 + c_3 l^3 m^3 + c_4 l^2 m^4 + c_5 l m^5 + c_6 m^6$$

where c_i are homogeneous polynomials of degree 4 in a, b, c, d, e, f.

Let

$$P_5(l,m) = Al^5 + Bl^4 m + Cl^3 m^2 + Dl^2 m^3 + Elm^4 + Fm^5, \tag{11}$$

where, without loss of generality (on multiplying $P_8(l,m)$ by a suitable constant), A, B, C, D, E, $F \in \mathbb{Z}$. Equating coefficients in (10) results after simple algebra in

$$A : B : C : D : E : F \tag{12}$$
$$= c_0\beta^5 : (c_0\alpha + c_1\beta)\beta^4 : (c_0\alpha^2 + c_1\alpha\beta + c_2\beta^2)\beta^3 :$$
$$(c_0\alpha^3 + c_1\alpha^2\beta + c_2\alpha\beta^2 + c_3\beta^3)\beta^2 :$$
$$(c_0\alpha^4 + c_1\alpha^3\beta + c_2\alpha^2\beta^2 + c_3\alpha\beta^3 + c_4\beta^4)\beta :$$
$$c_0\alpha^5 + c_1\alpha^4\beta + c_2\alpha^3\beta^2 + c_3\alpha^2\beta^3 + c_4\alpha\beta^4 + c_5\beta^5$$

with, from (10),

$$c_0\alpha^6 + c_1\alpha^5\beta + c_2\alpha^4\beta^2 + c_3\alpha^3\beta^3 + c_4\alpha^2\beta^4 + c_5\alpha\beta^5 + c_6\beta^6 = 0. \tag{13}$$

Now (13) is homogeneous of degree 4 in a, b, c, d, e, f and contains the factor $\pi(\alpha, \beta, \gamma, \delta)$ from (8). (Indeed, (13) factorizes as the product of the four linear terms $\pi(\alpha, \beta, \pm\gamma, \pm\delta)$ corresponding to the choice of $\nu_1'(T)$ as $(\alpha, \beta, \pm\gamma, \pm\delta)$. This remark is useful in numerical computation, allowing four choices of $\nu_1'(T)$ to be treated essentially simultaneously, with little extra computational effort.) Using the linear relation $\pi(\alpha, \beta, \gamma, \delta)$ to eliminate at (12) one of the quantities a, b, c, d, e, f results in $A : B : C : D : E : F$ being given as the ratios of six homogeneous quartic polynomials in five variables. For each choice of $\nu_1'(T)$, there will be a set of such polynomials. Provided these polynomials are algebraically independent, it is then possible successively to eliminate a, b, c, d, e, f resulting in an equation $P_{\mathrm{Big}}(A, B, C, D, E, F) = 0$; though in practice this may scarcely be possible. (Algebraic independence here is not clear. In the analogous situation of Cassels [2], there arise the ratios of four quadratics in $\mathbb{P}^2$, and independence is straightforward to verify by direct computation.)

Repeating the construction on E_j, $j = 2, \ldots, 5$, produces in each case a finite list of possibilities for $A : B : C : D : E : F$ as the ratio of homogeneous quartic polynomials in five variables. Accordingly, fixing a choice of $\nu_j'(T)$, $j = 1, \ldots, 5$, results in five expressions for $A : B : C : D : E : F$ as

the ratios of homogeneous quartics in $\mathbb{P}^4$. With algebraic independence, we could deduce five equations of type $P_{\mathrm{Big}(j)}(A,B,C,D,E,F)=0$. Assuming in turn that these equations are algebraically independent, they may then be solved for finitely many possible ratios $A:B:C:D:E:F$.

With $|C_j| = |G_j/2G_j| = 2^{g_j}$, there will be $\sum_{j=1}^{5} g_j$ choices for the $\nu_j'(T)$, and it is clear that to determine the pentuples T in practice will be an extremely laborious calculation, if indeed at all possible. In fact, the construction is more accessible to showing that there are *no* pentuples on E, which in a particular numerical example can be achieved without worrying about the algebraic independence of the systems of equations. We shall construct such an example (see Section 5) using local methods to prove that each set of five expressions for $A:B:C:D:E:F$ as the ratio of quartics in $\mathbb{P}^4$ is locally inconsistent for an appropriate prime p, so that there can be no simultaneous solution for $A:B:C:D:E:F$.

4. We give some arithmetical information about curves of the type E_i, which will be needed for the example of Section 5.

Let Γ denote the following elliptic curve:

$$\Gamma: \quad \begin{aligned} e_1x^2 + e_2y^2 &= z^2, \\ e_3x^2 + e_4y^2 &= w^2, \end{aligned} \qquad e_i \in \mathbb{Q};$$

with zero of $\Gamma(\mathbb{Q})$ being the point $O(x_0,y_0,z_0,w_0)$. We remark first that the hyperplane $e_3x_0x + e_4y_0y - w_0w = 0$ cuts out the divisor $2(x_0,y_0,z_0,w_0) + 2(x_0,y_0,-z_0,w_0)$. Denote by (p,q,r,s) a generic point of Γ.

Lemma 3. *The three points* $(x_0,y_0,-z_0,-w_0)$, $(x_0,-y_0,z_0,-w_0)$, $(x_0,-y_0,-z_0,w_0)$ *are of order* 2 *in* $\Gamma(\mathbb{Q})$, *and we have the following*:

$$\begin{aligned} (p,q,-r,-s) &= (p,q,r,s) + (x_0,y_0,-z_0,-w_0), \\ (p,-q,r,-s) &= (p,q,r,s) + (x_0,-y_0,z_0,-w_0), \\ (p,-q,-r,s) &= (p,q,r,s) + (x_0,-y_0,-z_0,w_0), \end{aligned} \tag{14}$$

where addition is that of $\Gamma(\mathbb{Q})$.

Proof. The function $(e_3px + e_4qy + sw)/(e_1px + e_2qy - rz)$ on Γ has divisor $2(p,q,-r,-s) - 2(p,q,r,s)$, from which $(x_0,y_0,-z_0,-w_0)$ has order 2 in $\Gamma(\mathbb{Q})$. Moreover, the function

$$\frac{(-sy_0 - qw_0)x + (sx_0 + pw_0)y + (-qx_0 + py_0)w}{(-ry_0 - qw_0)x + (rx_0 + pw_0)y + (qx_0 - py_0)z}$$

has divisor $(p,q,r,s) + (x_0,y_0,-z_0,-w_0) - (p,q,-r,-s) - (x_0,y_0,z_0,w_0)$, and hence the first equation in (14) follows. The other two equations follow mutatis mutandis. ∎

LEMMA 4.

$$\text{(15)}\quad \begin{aligned} &\text{(i) } (p,q,r,s)+(p,-q,r,s)=2(1,0,\sqrt{e_1},\sqrt{e_3}) \text{ in } \Gamma(\mathbb{Q}(\sqrt{e_1},\sqrt{e_3})),\\ &\text{(ii) } (p,q,r,s)+(-p,q,r,s)=2(0,1,\sqrt{e_2},\sqrt{e_4}) \text{ in } \Gamma(\mathbb{Q}(\sqrt{e_2},\sqrt{e_4})).\end{aligned}$$

P r o o f. The function $((\sqrt{e_3}z_0-\sqrt{e_1}w_0)x-(\sqrt{e_3}x_0-w_0)z+(\sqrt{e_1}x_0-z_0)w)$ cuts Γ in the divisor $2(1,0,\sqrt{e_1},\sqrt{e_3})+(x_0,y_0,z_0,w_0)+(x_0,-y_0,z_0,w_0)$, and the function $((sz_0-rw_0)x-(sx_0-pw_0)z+(rx_0-pz_0)w)$ in the divisor $(p,q,r,s)+(p,-q,r,s)+(x_0,y_0,z_0,w_0)+(x_0,-y_0,z_0,w_0)$; and (i) follows. By interchanging (e_1,e_3) with (e_2,e_4) and x with y, (ii) follows. ∎

LEMMA 5.

$$\text{(16)}\quad (x_0,y_0,-z_0,-w_0)=2((0,1,\sqrt{e_2},\sqrt{e_4})-(1,0,\sqrt{e_1},\sqrt{e_3})) \text{ in } \Gamma(\mathbb{Q}(\sqrt{e_1},\sqrt{e_2},\sqrt{e_3},\sqrt{e_4}).$$

P r o o f. The functions y and $(y(\sqrt{e_1e_4}+\sqrt{e_2e_3})-\sqrt{e_3}z-\sqrt{e_1}w)$ cut Γ in the divisors $(1,0,\pm\sqrt{e_1},\pm\sqrt{e_3})$ and $(1,0,\sqrt{e_1},-\sqrt{e_3})+(1,0,-\sqrt{e_1},\sqrt{e_3})+2(0,1,\sqrt{e_2},\sqrt{e_4})$, respectively; and it follows that $(1,0,\sqrt{e_1},\sqrt{e_3})+(1,0,-\sqrt{e_1},-\sqrt{e_3})=2(0,1,\sqrt{e_2},\sqrt{e_4})$ in $\Gamma(\mathbb{Q}(\sqrt{e_1},\sqrt{e_2},\sqrt{e_3},\sqrt{e_4}))$. But from the first equation at (14), $(1,0,-\sqrt{e_1},-\sqrt{e_3})=(1,0,\sqrt{e_1},\sqrt{e_3})+(x_0,y_0,-z_0,-w_0)$, and (16) now follows. ∎

Using (14)–(16), the following theorem is now immediate.

THEOREM 6. *Let* $(p,q,r,s)\in\Gamma(\mathbb{Q})$.

(i) *Suppose* e_1 *or* e_3 *is not a square in* $\mathbb{Q}$, *and* e_2 *or* e_4 *is not a square in* $\mathbb{Q}$. *Then the points* $(p,\pm q,\pm r,\pm s)\in\Gamma(\mathbb{Q})$ *represent eight distinct cosets in* $\Gamma(\mathbb{Q})/2\Gamma(\mathbb{Q})$.

(ii) *Suppose* $e_1,e_3\in\mathbb{Q}^{*2}$ *or* $e_2,e_4\in\mathbb{Q}^{*2}$, *but not both. Then the points* $(p,\pm q,\pm r,\pm s)\in\Gamma(\mathbb{Q})$ *represent precisely four distinct cosets in* $\Gamma(\mathbb{Q})/2\Gamma(\mathbb{Q})$.

(iii) *Suppose* $e_1,e_2,e_3,e_4\in\mathbb{Q}^{*2}$. *Then the points* $(p,\pm q,\pm r,\pm s)\in\Gamma(\mathbb{Q})$ *represent precisely two distinct cosets in* $\Gamma(\mathbb{Q})/2\Gamma(\mathbb{Q})$. ∎

5. An example. Consider the curve

$$\text{(17)}\quad \begin{aligned} E:\quad 4l^2-11m^2&=r^2,\\ 17l^2+m^2&=s^2,\\ l^2+m^2&=t^2,\end{aligned}$$

whose Jacobian is isogenous to the product of the following five curves of genus 1:

$$
\begin{aligned}
&E_1:\ 4l^2-11m^2=r^2, \quad E_2:\ 17l^2+m^2=s^2, \quad E_3:\ 4l^2-11m^2=r^2,\\
&\qquad 17l^2+m^2=s^2, \qquad\qquad l^2+m^2=t^2, \qquad\qquad l^2+m^2=t^2,\\
&E_4:\ 4s^2-191m^2=17r^2, \quad E_5:\ 191l^2-11s^2=r^2,\\
&\qquad s^2+16m^2=17t^2, \qquad\qquad -16l^2+s^2=t^2.
\end{aligned}
\tag{18}
$$

The E_i are elliptic curves, and we take as zeros of the respective groups

$$
\begin{aligned}
O_1(l,m,r,s) &= (1065,608,686,4433),\\
O_2(l,m,s,t) &= (0,1,1,1),\\
O_3(l,m,r,t) &= (1,0,2,1),\\
O_4(s,m,r,t) &= (16,1,7,4),\\
O_5(l,s,r,t) &= (6,25,1,7).
\end{aligned}
$$

In more traditional form, the E_i have equations

$$
\begin{aligned}
E_1:&\quad y^2=x(x+4)(x-187),\\
E_2:&\quad y^2=x(x+1)(x+17),\\
E_3:&\quad y^2=x(x+4)(x-11),\\
E_4:&\quad y^2=x(x+64)(x-191),\\
E_5:&\quad y^2=x(x+176)(x+191).
\end{aligned}
\tag{19}
$$

For interest, we give as illustration in the Appendix explicit maps between E_5 at (18) and E_5 at (19). Using a program such as Cremona's "mwrank" it is discovered that the rational rank of each E_i is equal to 1 with generators of infinite order $P_1\big(-\frac{4066304}{1134225}, \frac{20338462144}{1207949625}\big)$, $P_2(1,6)$, $P_3(16,40)$, $P_4(1024,30464)$, $P_5\big(\frac{16}{49}, \frac{36000}{343}\big)$, respectively. Equivalently, generators of infinite order on the curves (18) may be taken as $(1065,-608,686,4433)$, $(3,4,13,5)$, $(15,8,14,17)$, $(16,-1,7,4)$, $(6,-25,1,7)$ respectively. The torsion group in each case is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, of order 4.

THEOREM 7. (i) *E has points in $\mathbb{Q}_p$ for all primes p.*
(ii) *E has no points in $\mathbb{Q}$.*

Proof. (i) The curve E is singular only at 2, 11, 17 and so the Weil inequality mandates a point in $\mathbb{Q}_p$ for all primes $p \geq 101$. There is clearly a solution in $\mathbb{R}$ (completion at the infinite prime) with $m=0$; and it remains to find a solution in $\mathbb{Q}_p$ for primes $2 \leq p \leq 97$. Now 17 a p-adic square implies a p-adic point with $(l,m)=(1,0)$; and -11 a p-adic square implies a p-adic point with $(l,m)=(0,1)$. For the remaining primes, p-adic points are provided by the following table:

p	l	m	p	l	m
7	$\sqrt{15}$	1	41	3	1
11	2	1	61	8	1
17	$\sqrt{-1}$	1	73	13	1
29	8	1	79	1	1

(ii) A generator for the Mordell–Weil group $E_5(\mathbb{Q})$ of rank 1 is $P_5\big(\frac{16}{49}, \frac{36000}{343}\big)$, and the torsion group comprises the points $\{O, (0,0), (-191,0), (-176,0)\}$, where of course O denotes the zero of E_5 at (19).

Suppose that $(l,m,r,s,t) \in E(\mathbb{Q})$; by multiplying by a suitable integer, we may suppose $l,m,r,s,t \in \mathbb{Z}$ with $(l,m)=1$.

Now $P = \big(\frac{16r^2}{t^2}, \frac{240lrs}{t^3}\big) \in E_5(\mathbb{Q})$ so that $P = nP_5 + Q$ for some $n \in \mathbb{Z}$, and torsion point Q. Let $\phi : E_5(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ be the standard homomorphism (see Cassels [3], Lemma 14.2) defined here by $\phi([x,y]) = x \bmod \mathbb{Q}^{*2}$ for $x \neq 0$, $\phi(O) = 1 \bmod \mathbb{Q}^{*2}$, and $\phi([0,0]) = 176 \cdot 191 \bmod \mathbb{Q}^{*2}$. Then

$$1 = \phi(P) = \phi(nP_5 + Q) = \phi(P_5)^n \phi(Q) = \phi(Q) \bmod \mathbb{Q}^{*2},$$

forcing $Q = O$, and

$$\left(\frac{16r^2}{t^2}, \frac{240lrs}{t^3}\right) = n\left(\frac{16}{49}, \frac{36000}{343}\right).$$

Since E_5 is non-singular at 7, it follows that $7 \mid t$. But then, from (17), $l^2 + m^2 \equiv 0 \bmod 7$, implying $7 \mid l$, $7 \mid m$, a contradiction. ∎

THEOREM 8. *E has no points in any algebraic number field K of odd degree over $\mathbb{Q}$.*

Proof. From the introduction it suffices to show that E possesses no rational pentuple T of points. We follow the construction of Section 3; it is straightforward to verify using Section 4 that the following provide coset representatives for $E_j(\mathbb{Q})/2E_j(\mathbb{Q})$, $j = 1, \ldots, 5$:

$$\begin{aligned}
C_1 &= \{(1065, \pm 608, \pm 686, \pm 4433)\},\\
C_2 &= \{(0, 1, \pm 1, \pm 1), (3, 4\varepsilon_1, 13\varepsilon_2, 5\varepsilon_1\varepsilon_2)\},\\
C_3 &= \{(1, 0, \pm 2, \pm 1), (15, 8\varepsilon_1, 14\varepsilon_2, 17\varepsilon_1\varepsilon_2)\},\\
C_4 &= \{(16, \pm 1, \pm 7, \pm 4)\},\\
C_5 &= \{(6, \pm 25, \pm 1, \pm 7)\},
\end{aligned}$$

where $\varepsilon_1, \varepsilon_2 = \pm 1$.

Let A, B, C, D, E, F be as at (11); then from each E_j we obtain eight possibilities (according to the choice of $\nu_j'(T)$) for the ratios $A : B : C : D : E : F$, namely as

$$A : B : C : D : E : F = P_{j1}^{(k)} : P_{j2}^{(k)} : P_{j3}^{(k)} : P_{j4}^{(k)} : P_{j5}^{(k)} : P_{j6}^{(k)}, \quad j = 1, \ldots, 5, \quad k = 1, \ldots, 8, \tag{20}$$

where each $P_{jn}^{(k)}$ is homogeneous of degree 4 in $\mathbb{P}^4$. The elimination procedure is far too cumbersome to apply, and we resort to local arguments, in fact exclusively restricted to the prime 7.

A straightforward though tedious machine computation determines the set $R_j^{(k)}$ comprising all possible values for $A : B : C : D : E : F$ modulo 7, arising from the ratios at (20). Care is needed at this stage because in some instances the ratios become singular (delivering $0 : 0 : 0 : 0 : 0 : 0$) on a linear subvariety in $\mathbb{P}^4$, and it is necessary to apply an appropriate linear transformation on the underlying variables, followed by a repeat computation over $(\mathbb{Z}/7\mathbb{Z})^5$. The worst case occurred for $j = 1$ with the need to apply a linear transformation of determinant 7^{12}.

The upshot is the construction of sets $R_j^{(k)}$, which satisfy the following:

$$\begin{aligned}
&R_1^{(1)} = R_1^{(6)}, \quad R_1^{(2)} = R_1^{(5)}, \quad R_1^{(3)} = R_1^{(4)} = R_1^{(7)} = R_1^{(8)},\\
&R_2^{(1)} = R_2^{(2)} = R_2^{(3)} = R_2^{(4)}, \quad R_2^{(5)} = R_2^{(6)}, \quad R_2^{(7)} = R_2^{(8)},\\
&R_3^{(1)} = R_3^{(2)} = R_3^{(3)} = R_3^{(4)}, \quad R_3^{(5)} = R_3^{(6)}, \quad R_3^{(7)} = R_3^{(8)},\\
&R_4^{(1)} = R_4^{(2)} = R_4^{(5)} = R_4^{(6)}, \quad R_4^{(3)} = R_4^{(4)} = R_4^{(7)} = R_4^{(8)},\\
&R_5^{(1)} = R_5^{(2)} = R_5^{(5)} = R_5^{(6)}, \quad R_5^{(3)} = R_5^{(4)} = R_5^{(7)} = R_5^{(8)},
\end{aligned}$$

with orders given by

$$\begin{aligned}
&|R_1^{(k)}| = 595, \quad k = 1, \ldots, 8, \quad |R_2^{(k)}| = 927, \quad k = 1, \ldots, 8,\\
&|R_3^{(k)}| = 1007, \quad k = 1, \ldots, 4, \quad |R_3^{(k)}| = 645, \quad k = 5, \ldots, 8,\\
&|R_4^{(k)}| = 834, \quad k = 1, \ldots, 8, \quad |R_5^{(k)}| = 595, \quad k = 1, \ldots, 8.
\end{aligned}$$

And now $R_1^{(i_1)} \cap R_2^{(i_2)} \cap R_3^{(i_3)} \cap R_4^{(i_4)} \cap R_5^{(i_5)}$ is the empty set for all choices $1 \le i_k \le 8$, $k = 1, \ldots, 5$ (though there are only $3 \times 3 \times 3 \times 2 \times 2 = 108$ such intersections to check). Consequently, there is no common ratio $A : B : C : D : E : F$, and the theorem follows. ∎

Remarks. 1. Each polynomial $P_{jn}^{(k)}$ at (20) covers several computer screens, and the author appreciates that to check the above computation is no mean feat for the reader. The above details of the sets $R_j^{(k)}$ are provided as guideposts.

2. The curve at (17) seems particularly amenable to the above calculation. A first attempt at construction of an example used the curve

$$l^2 + m^2 = 2r^2, \quad 3l^2 - 2m^2 = s^2, \quad 3l^2 + m^2 = 244t^2$$

where again the rational rank of each curve E_i is at least 1. But several

weeks were spent on the local calculations at $p = 2, 3, 5, 7, 11$, which proved inconclusive; many of the $R_j^{(k)}$ intersections remained non-empty. The calculations for the example at (17) were performed on a SUN workstation, and took several hours.

Acknowledgements. I am grateful to the referee for correcting errors and suggesting ways in which to improve the presentation of this paper.

Appendix. Maps between the E_i at (18) and E_i at (19) are readily computed though are rather cumbersome. For example, when $i = 5$, we have the inverse maps

$$\begin{aligned}(x, y) = ((&1146l + r - 275s)(-96l + 25s + 7t)/(25l - 6s)^2,\\ &(-256704l^3 - 770224l^2 r + 64225l^2 s + 385350lrs + 15414ls^2\\ &- 48118rs^2 - 3850s^3 - 100657l^2 t + 56058lrt + 55050lst\\ &- 13450rst - 7414s^2 t)/(25l - 6s)^3),\end{aligned}$$

and

$$\begin{aligned}l : r : s : t = &\,20764401504 + 236160804x + 619806x^2 + 6x^3\\ &- 735350y - 3850xy :\\ &86518339600 + 906791600x + 2583275x^2 + 25x^3\\ &- 2823744y - 16044xy :\\ &- 3460733584 - 75598182x - 308847x^2 + x^3 + 66181500y :\\ &- 24225135088 + 705936x + 725781x^2 + 7x^3 - 4500xy.\end{aligned}$$

References

[1] A. Bremner, *Some quartic curves with no points in any cubic field*, Proc. London Math. Soc. (3) 52 (1986), 193–214.
[2] J. W. S. Cassels, *The arithmetic of certain quartic curves*, Proc. Roy. Soc. Edinburgh 100A (1985), 201–218.
[3] —, *Lectures on Elliptic Curves*, Cambridge University Press, 1991.
[4] W. Fulton, *Intersection Theory*, Springer, New York, 1984.

Department of Mathematics
Arizona State University
Tempe, Arizona 85287-1804
U.S.A.
E-mail: andrew@math.la.asu.edu

Received on 10.11.1995
and in revised form on 5.3.1996 (2892)