ACTA ARITHMETICA
LXXVII.4 (1996)

Explicit 4-descents on an elliptic curve

by

J. R. Merriman, S. Siksek and N. P. Smart (Canterbury)

1. Introduction. We wish to investigate how to find generators of an elliptic curve, $E(\mathbb{Q})$, modulo $2E(\mathbb{Q})$ defined over $\mathbb{Q}$. As is usual we can reduce this to the study of certain homogeneous spaces

$$y^2 = f(x, 1), \tag{1}$$

where $f(X, Z)$ is a binary quartic form (or quartic for short) with integer coefficients. One wishes to know whether equation (1) has a $\mathbb{Q}$-rational point and if so to exhibit one. One can often show that equation (1) has no $\mathbb{Q}$-rational points by local methods. However, even if (1) is everywhere locally soluble, it does not follow necessarily that a $\mathbb{Q}$-rational point exists; this failure of the "Hasse principle" is well known and gives rise to an element of the Tate–Shafarevich group.

Further, it is not necessarily the case that a rational point on equation (1) will have "small" coordinates. Hence searching for a rational point (even when one is known to exist) may be futile. This is important in some conditional algorithms, e.g. [13], for determining generators of E when one computes, for instance, the rank of the curve by assuming the conjectures of Birch and Swinnerton-Dyer. In such methods one then just needs to search for enough points with the correct regulator. One has a bound on the search region on the elliptic curve, but this can often be too large for practical use, especially if the curve has a generator with a large height. To get around this problem one could perform a 2-descent and then search in a bounded region on the descendants; this should be easier as this new region should be smaller. If however the search region is still too large, performing a further descent and obtaining a 4-descent will again reduce the search region, hopefully to something more manageable.

Interest in practical algorithms to find the generators of the Mordell–Weil group has grown in recent years due to the need to find the gener-

1991 *Mathematics Subject Classification*: Primary 11G05; Secondary 11Y16.
Key words and phrases: elliptic curves, Computational Number Theory.

ators to compute all the integral points using elliptic logarithms. This is the most efficient way known to compute integral points see ([23], [12], [21] and [22]).

In this paper we give an explicit method, suitable for machine calculation, to deal with such troublesome homogeneous spaces by considering further descents on equation (1). This has been done before in the literature (see [2] and [16]) for special types of elliptic curves. However, we could find no general account which was of use for systematic machine computations. We explain an explicit method for performing such further descents and we show this is equivalent to constructing elements of order dividing 4 in the Tate–Shafarevich group of the elliptic curve. Our method resembles that in [3] and [4]. The associated problem of finding generators of the Mordell–Weil group given generators of E/mE we shall not discuss here. However, a very efficient solution to this problem has recently been given by Siksek [18].

This work grew out of the PhD thesis [17] of the second author. However, it was not until John Cremona pointed out to us the link to us between classical invariant theory and 2-descents that we could see how to put everything together.

We would like to thank John Cremona and Nelson Stephens for their help and encouragement in the course of our work. We would also like to thank EPSRC who funded the research contained in this paper.

2. Background. Before we proceed to 4-descents we recap on the method of 2-descent. Let E be an elliptic curve over $\mathbb{Q}$ given by

$$Y^2 = X^3 + IX + J.$$

Now consider the set of all binary quartics with rational coefficients with the standard invariants I and J:

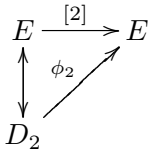
$$f = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4.$$

We only consider such quartics up to the relation of equivalence: f and g are equivalent if

$$g(x, z) = u^2 f(\alpha x + \beta z, \gamma x + \delta z)$$

for $u, \alpha, \beta, \gamma, \delta \in \mathbb{Q}$, with $u \neq 0$. It is well known (see [1]) that such quartics represent elements of the 2-Selmer group. They can be efficiently computed by the methods in [1] and [11].

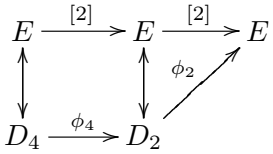
As the curves $D_2 : y^2 = f(x, z)$ are elements of the 2-Selmer group there is a map $\phi_2 : D_2 \to E$ defined over $\mathbb{Q}$ which commutes with the birational map from D_2 to its jacobian (which is E) and the multiplication by 2 map on E, i.e. we have the commutative diagram:



Given a rational point on D_2 and ϕ_2 we can compute its image on E. This is what one does in the standard method of 2-descent on an elliptic curve. By [10], one can take ϕ_2 to be the following map derived from the syzygy between the covariants of f. Let $H(x,z)$ denote the hessian determinant of $f(x,z)$ and $T(x,z)$ denote the Jacobian determinant of $f(x,z)$ and $H(x,z)$. Then we have

$$\phi_2(x,y) = (-H(x,1)/(4y^2), 3T(x,1)/(32y^3)).$$

Such curves $y^2 = f(x,1)$ correspond to elements of order dividing 2 in the Weil–Châtelet group of E. Now by [5], elements of order dividing 4 in $WC(E)$ correspond to curves D_4 whose jacobian is E and for which there is a map ϕ_4 defined over $\mathbb{Q}$ such that the following diagram is commutative:



Of course we are only interested in finding D_4's which cover a D_2 which is locally soluble everywhere. This could be for one of two reasons:

- To show that D_2 has no rational solutions and hence is an element of order 2 in the Tate–Shafarevich group of E.
- To produce a point on D_2 and hence via ϕ_2 produce a point on E.

This last reason is useful as the heights of rational points on D_4 should be much smaller than the height of equivalent points on D_2 and hence we expect them to be easier to find. In addition we will only be interested in D_2's which do not possess an obvious rational point. Hence we assume that either $f(x,z)$ is irreducible or that it is a product of two irreducible quadratic factors.

3. The intersection of two quadric surfaces. An element of order 4 in the Tate–Shafarevich group, Ш, of an elliptic curve will be represented by a principal homogeneous space $\mathcal{H}$ of period 4 and, by a well established result due to Lang and Tate (see for example [20, Exercise 10.11]), the index of this homogeneous space is also 4. This means that the minimum degree of a divisor on the curve, rational over $\mathbb{Q}$, is 4. We must therefore discuss the properties of curves of genus 1 with this property. Fortunately there is an excellent exposition in [26, Chapter 2, Appendix II], although we will

need to supplement this with some more detailed algebraic information. For convenience, we briefly summarise the geometry.

Suppose our divisor is Z_0. Then since $\mathcal{H}$ is a curve of genus 1, the linear system $|Z_0|$ is very ample and by Riemann–Roch has dimension 3. The image of $\mathcal{H}$ under the associated (bi-)rational mapping is therefore a non-singular quartic curve in $\mathbb{P}^3$. The projective coordinates x_1, x_2, x_3, x_4 cut out a basis for this linear system and, further, since the linear system $|2Z_0|$ has dimension 7 but contains the divisors corresponding to the 10 quadratic monomials $x_i x_j$, it is clear that $\mathcal{H}$ is contained in the intersection of two quadrics. Since $\mathcal{H}$ has genus 1 it is in fact a complete intersection of any pair of quadrics containing it. For convenience we will fix a pair, say $Q_1(\mathbf{x})$ and $Q_2(\mathbf{x})$, which we identify with their corresponding quadratic forms

$$Q_1(\mathbf{x}) = \mathbf{x}^t A\mathbf{x}, \qquad Q_2(\mathbf{x}) = \mathbf{x}^t B\mathbf{x}$$

where $\mathbf{x} = (x_1 : x_2 : x_3 : x_4)^t$. Hence $\mathcal{H}$ is given by the simultaneous equations $Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = 0$.

For any curve $\mathcal{X}$ one can construct a family of varieties $\mathrm{Pic}^n(\mathcal{X})$ parametrising divisor classes of degree n on $\mathcal{X}$. Thus, $\mathcal{J} = \mathrm{Pic}^0(\mathcal{X})$ is just the Jacobian variety of $\mathcal{X}$. Each $\mathrm{Pic}^n(\mathcal{X})$ for $n \geq 1$ is a principal homogeneous space for $\mathcal{J}$ and our next construction amounts to a birational identification of the curve $\mathrm{Pic}^2(\mathcal{H})$ for our curve $\mathcal{H}$ of genus 1. We consider the pencil of quadrics $Q_\lambda(\mathbf{x}) = \lambda_1 Q_1(\mathbf{x}) + \lambda_2 Q_2(\mathbf{x})$, for $\lambda = (\lambda_1 : \lambda_2) \in \mathbb{P}^1$, which contain $\mathcal{H}$ and let

$$F(\lambda) = F(\lambda_1, \lambda_2) = \det(\lambda_1 A + \lambda_2 B),$$

a homogeneous quartic polynomial in λ_1, λ_2. This defines a curve of genus 1 which is the double covering of $\mathbb{P}^1$ ramified at the 4 points corresponding to the zeros of F. The coefficients of $F(\lambda_1, \lambda_2)$ are the basic invariants of $Q_1(\mathbf{x})$ and $Q_2(\mathbf{x})$ (see below) and we denote by D_2 the curve $Y^2 = F(\lambda_1, 1)$. Using the notation of [26, Appendix III] we can construct a rational mapping (defined over $\mathbb{Q}$)

$$\omega : \mathcal{H} \times \mathcal{H} \to D_2$$

by the recipe: if P_1, P_2 denote points of $\mathcal{H}$ there is a unique point $\lambda = (\lambda_1 : \lambda_2) \in \mathbb{P}^1$ such that the line P_1P_2 (tangent if $P_1 = P_2$) lies in the quadric Q_λ. As explained in [26, Appendix III], $F(\lambda_1, \lambda_2)$ is a square and hence we obtain a point, $\omega(P_1, P_2)$, on the double cover. This construction yields a rational mapping with the properties

$$\omega(P_1, P_2) = \omega(P_1', P_2') \Leftrightarrow P_1 + P_2 \sim P_1' + P_2'$$

and therefore induces a birational mapping of $\mathrm{Pic}^2(\mathcal{H})$ with D_2. When we fix a point on $\mathcal{H}$, say P_0, the mapping $P \mapsto \omega(P, P_0)$ induces a birational map between $D_2 \times_{\mathbb{Q}} \mathbb{Q}(P_0)$ and $\mathcal{H} \times_{\mathbb{Q}} \mathbb{Q}(P_0)$ and both are identified with the elliptic curve which is their Jacobian over $\mathbb{Q}(P_0)$, i.e. $\mathcal{J} \times_{\mathbb{Q}} \mathbb{Q}(P_0)$. Were

$\mathcal{H}$ to have a $\mathbb{Q}$-rational divisor of degree 2 then $\mathrm{Pic}^2(\mathcal{H}) \simeq \mathrm{Pic}^0(\mathcal{H})$ and $\mathcal{H}$ would correspond to a 2-covering of $\mathcal{J}$ and so correspond to an element of order dividing 2 in Ш.

We now assume that a point P_0 on $\mathcal{H}$ has been fixed and assume we are working over a field of definition for $\mathcal{H}$ and P_0. Then $\mathcal{H}$ itself has the structure of an elliptic curve isomorphic to that of its Jacobian.

Geometrically the group law is given as follows: P_1, P_2, P_3 have the properties

$$P_1 + P_2 + P_3 = 0 \Leftrightarrow P_0, P_1, P_2, P_3 \text{ are coplanar.}$$

Further $-P_1$ is the residual intersection of the plane through P_1 containing the tangent line to $\mathcal{H}$ at P_0. From this description it is then clear that points of order 2 on $\mathcal{H}$ are those points at which the tangent line to $\mathcal{H}$ is coplanar with the tangent line at P_0. If P_1 denotes such a point, a simple geometrical argument shows that the unique quadric in the pencil Q_λ which contains the line P_0P_1 must be a cone and this is precisely the condition that $F(\lambda) = 0$, i.e. $\omega(P_1, P_0)$ is a ramification point of the double covering $D_2 \to \mathbb{P}^1$.

We now turn our attention to the invariant theory of our pair of quadric surfaces in $\mathbb{P}^3$. Much of what follows will be found in Todd, [25, Chapter 7], but using a different notation. As above let

$$Q_1(\mathbf{x}) = \mathbf{x}^t A\mathbf{x}, \qquad Q_2(\mathbf{x}) = \mathbf{x}^t B\mathbf{x},$$

where A and B are two symmetric 4×4 matrices, denote our two quadric surfaces with transversal intersection. We then define the basic invariants, $\sigma_0, \ldots, \sigma_4$, of $Q_1(\mathbf{x})$ and $Q_2(\mathbf{x})$ by the equation

$$\det(t_1A + t_2B) = t_1^4\sigma_0 + t_1^3t_2\sigma_1 + t_1^2t_2^2\sigma_2 + t_1t_2^3\sigma_3 + t_2^4\sigma_4.$$

To determine the fundamental covariants we first set $A' = \mathrm{adj}(A)$, $B' = \mathrm{adj}(B)$ and then define d_1 and d_2 to be the two symmetric matrices determined by

$$\mathrm{adj}(t_1A' + t_2B') = t_1^3\sigma_0^2A + t_1^2t_2\sigma_0d_1 + t_1t_2^2\sigma_4d_2 + t_2^3\sigma_4^2B.$$

We then define two more quadratic forms

$$F_1(\mathbf{x}) = \mathbf{x}^t d_1\mathbf{x}, \qquad F_2(\mathbf{x}) = \mathbf{x}^t d_2\mathbf{x}.$$

The five fundamental covariants of $Q_1(\mathbf{x})$ and $Q_2(\mathbf{x})$ are then given by $Q_1(\mathbf{x})$, $Q_2(\mathbf{x})$, $F_1(\mathbf{x})$, $F_2(\mathbf{x})$ and the jacobian

$$G(\mathbf{x}) = \frac{1}{16}\frac{\partial(Q_1, Q_2, F_1, F_2)}{\partial(x_1, x_2, x_3, x_4)}.$$

LEMMA 1. *The invariants σ_i and the covariants $F_1(\mathbf{x})$, $F_2(\mathbf{x})$ are of weight two, the covariants $Q_1(\mathbf{x})$ and $Q_2(\mathbf{x})$ are of weight zero, whilst the covariant $G(\mathbf{x})$ is of weight 5.*

P r o o f. Let $\mathbf{x} = T\mathbf{y}$ denote a change of variable. Putting $U^t = \mathrm{adj}(T)$ we have

$$\mathrm{adj}(U^t) = \mathrm{adj}((\det T)T^{-1}) = (\det T)^2 T.$$

Let $A^* = T^t A T$, $A'^* = U^t A' U$ etc. Then we have

- The invariants σ_i have weight two because

$$\det(t_1 A^* + t_2 B^*) = (\det T)^2 \det(t_1 A + t_2 B).$$

- The covariants $Q_1(\mathbf{x})$ and $Q_2(\mathbf{x})$ have weight zero because

$$Q_1^*(\mathbf{y}) = \mathbf{y}^t A^* \mathbf{y} = \mathbf{y}^t T^t A T \mathbf{y} = \mathbf{x}^t A \mathbf{x} = Q_1(\mathbf{x}).$$

- The covariants $F_1(\mathbf{x})$ and $F_2(\mathbf{x})$ are of weight two because

$$\mathrm{adj}(t_1 A'^* + t_2 B'^*) = (\det T)^4 \,\mathrm{adj}(t_1 A' + t_2 B')$$

and so $\sigma_0^* d_1^* = (\det T)^4 \sigma_0 T^t d_1 T$. Hence $d_1^* = (\det T)^2 T^t d_1 T$. Similarly for d_2.

- The fact that the covariant $G(\mathbf{x})$ has weight 5 then follows from the definition by applying the rule for computing the partial derivatives of a composition of functions. ∎

One then finds that the syzygy given by

$$\begin{aligned}(*)\quad & {F_2}^2 Q_1 Q_2 \sigma_1 {\sigma_3}^2 - 2{F_2}^2 Q_1 Q_2 \sigma_1 \sigma_2 \sigma_4 + {F_2}^3 Q_2 \sigma_1 \sigma_4 - 2{\sigma_0}^2 {F_1}^2 {Q_2}^2 \sigma_4 \\
& -3{\sigma_0}^2 {Q_1}^2 {Q_2}^2 {\sigma_3}^2 \sigma_4 - 3\sigma_0 {F_1}^2 F_2 Q_2 \sigma_3 - {F_2}^3 Q_1 {\sigma_3}^2 \\
& + \sigma_0 F_1 {Q_1}^2 Q_2 \sigma_1 \sigma_3 \sigma_4 - \sigma_0 {F_1}^2 {Q_2}^2 {\sigma_2}^2 + 3{\sigma_0}^2 {Q_1}^2 {Q_2}^2 \sigma_2 {\sigma_4}^2 + 2{F_2}^3 Q_1 \sigma_2 \sigma_4 \\
& - 2\sigma_0 {F_1}^2 Q_1 Q_2 \sigma_2 \sigma_3 + {F_1}^2 F_2 Q_2 \sigma_1 \sigma_2 - {F_2}^4 \sigma_4 - \sigma_0 {Q_1}^2 {Q_2}^2 {\sigma_2}^3 \sigma_4 \\
& + 4\sigma_0 {F_1}^2 F_2 Q_1 \sigma_4 - {F_1}^2 F_2 Q_1 \sigma_1 \sigma_3 + 2{\sigma_0}^2 F_1 {Q_2}^3 \sigma_2 \sigma_4 - \sigma_0 {F_1}^2 Q_1 Q_2 \sigma_1 \sigma_4 \\
& + 2\sigma_0 {F_1}^2 {Q_2}^2 \sigma_1 \sigma_3 - {\sigma_0}^2 F_1 {Q_2}^3 {\sigma_3}^2 + 3\sigma_0 {Q_1}^2 {Q_2}^2 \sigma_1 \sigma_2 \sigma_3 \sigma_4 + 2\sigma_0 {F_1}^3 Q_2 \sigma_2 \\
& - \sigma_0 F_2 {Q_1}^2 Q_2 \sigma_2 \sigma_3 \sigma_4 + 3{\sigma_0}^2 {Q_1}^3 Q_2 \sigma_3 {\sigma_4}^2 - {F_1}^3 Q_2 {\sigma_1}^2 + \sigma_0 {F_1}^3 Q_1 \sigma_3 \\
& + 5\sigma_0 F_2 {Q_1}^2 Q_2 \sigma_1 {\sigma_4}^2 + 4\sigma_0 F_1 {F_2}^2 Q_2 \sigma_4 + {F_1}^3 F_2 \sigma_1 - \sigma_0 {F_1}^4 \\
& + F_2 {Q_1}^2 Q_2 \sigma_1 {\sigma_2}^2 \sigma_4 + \sigma_0 F_1 F_2 {Q_2}^2 \sigma_2 \sigma_3 - F_1 {F_2}^2 Q_2 \sigma_1 \sigma_3 - 3\sigma_0 {Q_1}^2 {Q_2}^2 {\sigma_1}^2 {\sigma_4}^2 \\
& - 3\sigma_0 F_1 F_2 {Q_2}^2 \sigma_1 \sigma_4 - 3\sigma_0 {Q_1}^3 Q_2 \sigma_1 \sigma_2 {\sigma_4}^2 - 4{\sigma_0}^2 F_1 {Q_1}^2 Q_2 {\sigma_4}^2 \\
& + F_1 {F_2}^2 Q_1 \sigma_2 \sigma_3 + 2\sigma_0 F_1 {Q_1}^2 Q_2 {\sigma_2}^2 \sigma_4 - \sigma_0 {F_2}^2 {Q_2}^2 \sigma_2 \sigma_4 + {\sigma_0}^2 F_2 {Q_2}^3 \sigma_3 \sigma_4 \\
& + {F_1}^2 Q_1 Q_2 {\sigma_1}^2 \sigma_3 - 3F_1 {F_2}^2 Q_1 \sigma_1 \sigma_4 - 4{\sigma_0}^2 F_2 Q_1 {Q_2}^2 {\sigma_4}^2 + F_1 {F_2}^3 \sigma_3 \\
& - 2F_2 {Q_1}^2 Q_2 {\sigma_1}^2 \sigma_3 \sigma_4 - \sigma_0 F_2 Q_1 {Q_2}^2 \sigma_2 {\sigma_3}^2 - F_1 {Q_1}^2 Q_2 {\sigma_1}^2 \sigma_2 \sigma_4 \\
& + 2\sigma_0 F_2 Q_1 {Q_2}^2 {\sigma_2}^2 \sigma_4 - 2\sigma_0 {F_2}^2 {Q_1}^2 {\sigma_4}^2 - {F_2}^2 {Q_1}^2 {\sigma_2}^2 \sigma_4 + 3\sigma_0 F_1 F_2 Q_1 Q_2 {\sigma_3}^2 \\
& + \sigma_0 F_2 Q_1 {Q_2}^2 \sigma_1 \sigma_3 \sigma_4 - \sigma_0 {F_2}^2 Q_1 Q_2 \sigma_3 \sigma_4 - 4\sigma_0 F_1 F_2 Q_1 Q_2 \sigma_2 \sigma_4 \\
& + 2{F_2}^2 {Q_1}^2 \sigma_1 \sigma_3 \sigma_4 - \sigma_0 {F_1}^2 {Q_1}^2 \sigma_2 \sigma_4 + {Q_1}^3 Q_2 {\sigma_1}^3 {\sigma_4}^2 - {\sigma_0}^2 {Q_1}^4 {\sigma_4}^3 \\
& - {\sigma_0}^3 {Q_2}^4 {\sigma_4}^2 - F_1 F_2 Q_1 Q_2 \sigma_1 \sigma_2 \sigma_3 + 5{\sigma_0}^2 F_1 Q_1 {Q_2}^2 \sigma_3 \sigma_4 + \sigma_0 F_1 Q_1 {Q_2}^2 {\sigma_2}^2 \sigma_3 \\
& + \sigma_0 F_1 {Q_1}^3 \sigma_1 {\sigma_4}^2 + 3F_1 F_2 Q_1 Q_2 {\sigma_1}^2 \sigma_4 + 2\sigma_0 F_2 {Q_1}^3 \sigma_2 {\sigma_4}^2\end{aligned}$$

$$-2\sigma_0 F_1 Q_1 {Q_2}^2 \sigma_1 {\sigma_3}^2 - \sigma_0 F_1 Q_1 {Q_2}^2 \sigma_1 \sigma_2 \sigma_4 - 3{\sigma_0}^2 Q_1 {Q_2}^3 \sigma_2 \sigma_3 \sigma_4$$
$$-3\sigma_0 F_1 F_2 {Q_1}^2 \sigma_3 \sigma_4 + {\sigma_0}^2 Q_1 {Q_2}^3 {\sigma_3}^3 - {F_1}^2 {F_2}^2 \sigma_2 + F_1 F_2 {Q_1}^2 \sigma_1 \sigma_2 \sigma_4$$
$$-F_2 {Q_1}^3 {\sigma_1}^2 {\sigma_4}^2 + 3{\sigma_0}^2 Q_1 {Q_2}^3 \sigma_1 {\sigma_4}^2 + G^2 = 0$$

holds. This was derived by applying the above weight considerations to the two quadrics

$$Q_1(\mathbf{x}) = \mu_1 x_1^2 + \mu_2 x_2^2 + \mu_3 x_3^2 + \mu_4 x_4^2, \qquad Q_2(\mathbf{x}) = \lambda_1 x_1^2 + \lambda_2 x_2^2 + \lambda_3 x_3^2 + \lambda_4 x_4^2.$$

By a linear change of variable defined over $\mathbb{C}$ one can always put our two quadrics in this form as we have assumed that they are transversal. As it is a formal identity holding for these two quadrics it must then hold in general.

When $\mathbf{x}$ is a point on our intersection of two quadrics the syzygy $(*)$ reduces to

$$G^2 = \sigma_0 {F_1}^4 - {F_1}^3 F_2 \sigma_1 + {F_1}^2 {F_2}^2 \sigma_2 - F_1 {F_2}^3 \sigma_3 + {F_2}^4 \sigma_4.$$

So we have a map from $\mathcal{H}$ onto a curve of the form

$$D_2 : y^2 = \sigma_0 x^4 + \sigma_1 x^3 + \sigma_2 x^2 + \sigma_3 x + \sigma_4$$

given by

$$\psi : \begin{array}{l} \mathcal{H} \to D_2, \\ \mathbf{x} \to (-F_1(\mathbf{x})/F_2(\mathbf{x}), G(\mathbf{x})/F_2(\mathbf{x})^2). \end{array}$$

Now if D_2 were a two-covering of an elliptic curve E, then the map above would correspond to a map ϕ_4, i.e. an extension of the two-covering to a four-covering, if we could show the following:

- The map ψ above has degree 4.
- Let P_0 denote a point on D_2 with zero y-coordinate, and let $P_1, \ldots, P_4$ denote the pre-images of P_0 under ψ. If we choose P_1 as a zero of the group law on $\mathcal{H}$ then P_2, P_3, P_4 are the points of order two.

In other words, if we consider D_2 as an elliptic curve with base point P_0 then the following diagram is commutative:

$$\begin{array}{ccc} (D_2, P_0) & \xrightarrow{[2]} & (D_2, P_0) \\ \uparrow\downarrow & \nearrow_{\psi} & \\ \mathcal{H} & & \end{array}$$

The fact that ψ is a degree 4 map can be seen by considering a point (x, y, z) on D_2. Then the point $\mathbf{x}$ lies on the three quadric surfaces

$$Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = zF_1(\mathbf{x}) + xF_2(\mathbf{x}) = 0.$$

By Bezout's Theorem these intersect in eight points and the imposition of the condition $G(\mathbf{x}) = y$ determines a subset of four points.

Now the condition that the images of the four points $P_1, \dots, P_4$ have zero y coordinate means that $G(\mathbf{x}) = 0$. But this means that the four points lie on the union of four planes in $\mathbb{P}^3$ (to see this consider Todd, [25, p. 249]). However, as the images of the four points are equal, the ratio of $F_1(\mathbf{x})$ and $F_2(\mathbf{x})$ is constant and so the four points all lie on the same plane. Now consider a plane which contains the tangent at P_1 and which also passes through P_i, for $2 \le i \le 3$. Then, if P_i is not a point of order two, such a plane intersects $\mathcal{H}$ in one other (distinct) point (see our discussion on the group law above). But then it would be a plane which contained $P_1, \dots, P_4$ and the tangent line at P_1, which is impossible. Hence P_i is a point of order two.

4. The descent construction. We wish to parametrise the solutions to equation (1) over $\mathbb{Q}$. By a change of variable we can assume our homogeneous space is of the form

$$\mathcal{C} : aY^2 = G(X, Z), \tag{2}$$

where $G(X, Z)$ is a binary quartic form with $\mathbb{Z}$ coefficients, with $G(1, 0) = 1$ and $a \in \mathbb{Q}^*$ is the coefficient of x^4 in $f(x, z)$. We wish to determine (X, Z) up to multiplication by an element of $\mathbb{Q}^*$ and so we can assume that $(X, Z) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ and (X, Z) are coprime. Let $A = \mathbb{Q}[\Theta]$ denote the algebra

$$\mathbb{Q}[X]/(G(X, 1)) = L_1 \oplus \ldots \oplus L_t,$$

where the L_i are number fields such that $L_i = \mathbb{Q}(\theta_i)$ and $G(\theta_i, 1) = 0$ and no two distinct pairs θ_i, θ_j are conjugate. We can hence assume, as $G(X, Z)$ is irreducible or a product of two irreducible quadratic factors, that $t = 1$ or 2. Put $(X - \theta_i Z)\mathcal{O}_{L_i} = \mathfrak{a}_i \mathfrak{b}_i^2$, where $\mathfrak{a}_i$ is square free and $\prod_{i=1}^{t} N_{L_i/\mathbb{Q}}(\mathfrak{a}_i) \in a\mathbb{Q}^{*2}$.

Lemma 2. *If $\mathfrak{p}$ is a prime ideal of L_i and $\mathfrak{p} \mid \mathfrak{a}_i$ then either $\mathfrak{p} \mid a$, or $\mathfrak{p} \mid \Delta(G)$, where $\Delta(G)$ is the discriminant of $G(X, Z)$*

Proof. Suppose $\mathfrak{p}$ is a prime ideal of L_i such that $\mathfrak{p}|\mathfrak{a}$ but $\mathfrak{p}$ does not divide a or $\Delta(G)$. Let L^{Gal} denote the minimal Galois closure of $L_1 \cup \ldots \cup L_t$. As $\mathfrak{p}$ does not divide $\Delta(G)$ we see that $\mathfrak{p}$ does not ramify in L^{Gal}. Let $\mathfrak{q}$ denote a prime ideal of L^{Gal} which divides $\mathfrak{p}$. Then

$$\mathrm{ord}_{\mathfrak{q}}(X - \theta_i Z) = \mathrm{ord}_{\mathfrak{p}}(X - \theta_i Z) \equiv 1 \pmod 2,$$

as $\mathfrak{a}_i$ is square free. But

$$\mathrm{ord}_{\mathfrak{q}}\Big(\prod_{i=1}^{t} N_{L_i/\mathbb{Q}}(X - \theta_i Z)\Big) = \mathrm{ord}_{\mathfrak{q}} G(X, Z) = \mathrm{ord}_{\mathfrak{q}}(aY^2) \equiv 0 \pmod 2,$$

as $\mathfrak{q}$ does not divide a.

So there is a θ with $G(\theta,1)=0$ such that $\theta\neq\theta_i$ and $\mathfrak{q}\,|\,(X-\theta Y)$. Then we find that $\mathfrak{q}$ divides $(\theta-\theta_i)X$ and $(\theta-\theta_i)Z$. But as $\mathfrak{q}$ does not divide $\theta-\theta_i$ we find that $\mathfrak{q}\,|\,(X,Z)$. But this is true for all prime ideals $\mathfrak{q}$ of L^{Gal} which divide $\mathfrak{p}$, hence $\mathfrak{p}\,|\,(X,Z)$. But this means that $\mathfrak{p}$ is the trivial ideal. ∎

Let S_i denote the set of prime ideals in L_i which divide a or $\Delta(G)$. We let $L_i(S_i,2)$ denote the set of elements of L_i modulo squares such that if we add a square root of an element of $L_i(S_i,2)$ to L_i we obtain an extension unramified away from S_i. This finite set can be determined by the methods of [19]. Using the above lemma we can then write

$$X-\theta_i Z=\varepsilon_i\gamma_i^2, \tag{3}$$

where $\varepsilon_i\in L_i(S_i,2)$ and $\gamma_i\in L_i^*$. For each tuple $(\varepsilon_1,\dots,\varepsilon_t)$ we reject those for which

$$\prod_{i=1}^{t} N_{L_i/\mathbb{Q}}(\varepsilon_i)\notin a\mathbb{Q}^{*2}.$$

We can obviously assume that $(\varepsilon_1,\dots,\varepsilon_t)$ is determined modulo an element of $\mathbb{Q}^*$. We then have a map

$$\mu:\begin{array}{ccc}\mathcal{C} & \to & A^*/\mathbb{Q}^*A^{*2},\\ (X,Y,1) & \to & X-\Theta Z \pmod{\mathbb{Q}^*A^{*2}},\end{array}$$

which should be familiar as the usual map one uses to perform 2-descents on a curve of the form (1) when $f(x,z)$ is monic (see [6]).

We finally obtain a finite set of equations of the form (3); from each one of these sets of equations we shall derive the descendants. We now look at the two various cases corresponding to the factorization of $G(X,Z)$. In all cases we obtain a new "homogeneous space" as an intersection of two quadrics.

4.1. *$G(X,Z)$ is irreducible.* For convenience we make the change of variable such that the coefficient of X^3Z in $G(X,Z)$ is zero. We have the equation

$$X-\theta Z=\varepsilon(x_1+x_2\theta+x_3\theta^2+x_4\theta^3)^2$$

from which we obtain (on equating coefficients of θ^j) the four equations

$$X=Q_3(\mathbf{x}),\quad Z=Q_4(\mathbf{x}),\quad 0=Q_1(\mathbf{x}),\quad 0=Q_2(\mathbf{x}),$$

where $Q_i(\mathbf{x})$ is a quadratic form in four variables. The last two equations give us our two quadrics.

Given the above change of variable, one can easily check that if $F_1(\mathbf{x})$ and $F_2(\mathbf{x})$ denote the corresponding covariants of $Q_1(\mathbf{x})$ and $Q_2(\mathbf{x})$ then a point $\mathbf{x}$ such that $Q_1(\mathbf{x})=Q_2(\mathbf{x})=0$ satisfies the identities

$$Q_3(\mathbf{x})\equiv F_1(\mathbf{x}),\qquad Q_4(\mathbf{x})\equiv -F_2(\mathbf{x}).$$

And in addition

$$\det(Q_1(\mathbf{x})t_1 + Q_2(\mathbf{x})t_2) = aG(t_1, t_2).$$

Hence in this case the above construction does indeed give rise to a 4-descent extending the 2-descent (1).

4.2. *$G(X, Z)$ is a product of two irreducible quadratics.* Here we find the equations

$$X - \theta_1 Z = \varepsilon_1(x_1 + \theta_1 x_2)^2, \quad X - \theta_2 Z = \varepsilon_2(x_3 + \theta_2 x_4)^2.$$

Again equating coefficients of θ_1 we find the X (resp. Z) in terms of two different quadratic forms. Then equating coefficients of θ_2 we find two quadrics $Q_1(\mathbf{x})$ and $Q_2(\mathbf{x})$ which must be equal to zero. Again we find

$$\det(Q_1(\mathbf{x})t_1 + Q_2(\mathbf{x})t_2) = aG(t_1, t_2).$$

But this time for a point $\mathbf{x}$ satisfying $Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = 0$ we find that

$$X(\mathbf{x}) \equiv c_1F_1(\mathbf{x}) + c_2F_2(\mathbf{x}), \quad Z(\mathbf{x}) \equiv c_3F_1(\mathbf{x}) + c_4F_2(\mathbf{x})$$

for some constants c_i depending only on the coefficients of $G(t_1, t_2)$. However, we then notice that

$$G(c_1F_1(\mathbf{x}) + c_2F_2(\mathbf{x}), c_3F_1(\mathbf{x}) + c_4F_2(\mathbf{x})) = G(F_1(\mathbf{x}), -F_2(\mathbf{x}))/\delta^2,$$

where δ is also some constant depending only on the coefficients of $G(t_1, t_2)$. Hence in this case we also find that the above construction does produce a 4-descent extending the 2-descent (1).

We now discard every 4-descent which is not locally soluble everywhere. To do this we need to test whether the intersection of two quadrics is soluble in every completion of $\mathbb{Q}$. However, we note the following result which can often speed up this search, given that the methods below for local solubility are quite cumbersome. We shall denote by A_p the obvious localisation of the algebra A.

LEMMA 3. *Suppose we know that equation* (2) *has three solutions over $\mathbb{Q}_p$, say P_1, P_2 and P_3. (This may be because we know that some element in $L_1(S_1, 2) \times \ldots \times L_t(S_t, 2)$ gives rise to an intersection of two quadrics that we know to be soluble in $\mathbb{Q}_p$ by the methods below.) Suppose the curve*

$$Y = b_2X^2 + b_1XZ + b_0Z^2$$

intersects (2) *at the three points P_1, P_2, P_3. Then the fourth point of intersection, P_4, is also defined over $\mathbb{Q}_p$ and we have*

$$\prod_{i=1}^{4} \mu(P_i) \equiv 1 \pmod{A_p^*/Q_p^*A_p^{*2}}.$$

P r o o f. That P_4 is also defined over $\mathbb{Q}_p$ is obvious. For the other part we set $X = \Theta$ on both sides of the identity

$$a(b_2X^2 + b_1X + b_0)^2 - G(X,1) = l(X - x(P_1))\dots(X - x(P_4)). \blacksquare$$

5. Local solubility of an intersection of two quadrics. We first consider the non-archimedean case, then we shall go onto the archimedean case.

5.1. *The non-archimedean case.* We let v denote the non-archimedean valuation of $\mathbb{Q}$ we shall be considering, p the corresponding prime number and $\mathbb{P}_p = \{(x:y) : x, y \in \mathbb{Z}_p \text{ and } \min(v(x), v(y)) = 0\}$.

Let A, B be 4×4 symmetric matrices with entries in $\mathbb{Q}$ such that $\det(XA - YB)$ has distinct roots. We shall give an algorithm for determining the solubility of

$$\mathcal{H} : \begin{cases} \mathbf{x}^t A\mathbf{x} = 0, \\ \mathbf{x}^t B\mathbf{x} = 0 \end{cases}$$

over $\mathbb{Q}_p$. We can assume without loss of generality that A and B have entries in $\mathbb{Z}$ and hence that $\partial(A,B)$ (the discriminant of $\det(XA - YB)$) is in $\mathbb{Z}$.

The algorithm we will give relies on searching for points on $\mathcal{H}$ modulo p and then attempting to lift the points found to points modulo powers of p until it is certain that they will lift to points defined over $\mathbb{Z}_p^4$. We need two pieces of information:

1. For which of the infinitely many $v \in M_{\mathbb{Q}}^0$ is it necessary to do this?
2. Modulo which power of the corresponding p is it sufficient to find a solution, to be sure that this solution will lift?

Theorem 4. *Suppose A, B are 4×4 symmetric matrices with entries in $\mathbb{Z}_p$ such that $\partial(A,B) \neq 0$. We have*

1. *If $v(2\partial(A,B)) = 0$ then $\mathcal{H}$ has a non-trivial solution over $\mathbb{Z}_p$.*
2. *Suppose that there exists $\mathbf{x}_0 \in \mathbb{Z}_p^4 \backslash p\mathbb{Z}_p^4$ such that*

$$\mathbf{x}_0^t A\mathbf{x}_0 \equiv \mathbf{x}_0^t B\mathbf{x}_0 \equiv 0 \pmod{p^{2\delta+1}}$$

and there is no pair $(\lambda:\mu) \in \mathbb{P}_p$ such that $2(\lambda A\mathbf{x}_0 - \mu B\mathbf{x}_0) \equiv \mathbf{0} \pmod{p^{\delta+1}}$. Then there exists $\mathbf{x} \in \mathbb{Z}_p^4$ such that $\mathbf{x} \equiv \mathbf{x}_0 \pmod{p^{\delta+1}}$ and $\mathbf{x}$ is a non-trivial point on $\mathcal{H}$.

P r o o f. For the first part it is sufficient to note that if $v(2\partial(A,B)) = 0$ then $\mathbf{x}^t\overline{A}\mathbf{x} \equiv \mathbf{x}^t\overline{B}\mathbf{x} \equiv 0 \pmod{p}$ has genus 1 and it then follows that there is a non-trivial solution to $\mathcal{H}$. The second part is a special case of Theorem 5.21 on page 64 of [14]. $\blacksquare$

Thus it is clear that to test local solubility at the non-archimedean places, it is sufficient to check solubility over $\mathbb{Q}_p$ only for those p for which $v(2\partial(A,B))$ is not equal to 0. For any such p, we can do this using the

above theorem in a standard way (cf. the book [11] where a similar algorithm is given for the case $y^2 = f(x,1)$). That such a process terminates is guaranteed by the following lemma.

LEMMA 5. *Suppose that there exists* $\mathbf{x}_1 \in \mathbb{Z}_p^4$ *such that*

$$\mathbf{x}_1 A \mathbf{x}_1 \equiv \mathbf{x}_1 B \mathbf{x}_1 \equiv 0 \pmod{p^\alpha}$$

and there exists $(\lambda : \mu) \in \mathbb{P}_p$ *such that* $(\lambda A\mathbf{x}_1 - \mu B\mathbf{x}_1) \equiv \mathbf{0} \pmod{p^\beta}$. *Then* $\min(\alpha, \beta) \le v(\partial(A, B))$.

Proof. Let $\gamma = \min(\alpha, \beta)$. Choose $\mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4 \in \mathbb{Z}_p^4$ such that $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4$ are linearly independent modulo p. Let T be the 4×4 matrix with columns $\mathbf{x}_1,\ \mathbf{x}_2,\ \mathbf{x}_3,\ \mathbf{x}_4$. Further, choose $(\lambda' : \mu') \in \mathbb{P}_p$ such that $\lambda\mu' - \lambda'\mu \not\equiv 0 \pmod{p}$. Write

$$C = T^t(\lambda A - \mu B)T, \qquad D = T^t(\lambda' A - \mu' B)T.$$

Then $v(\partial(C, D)) = v(\partial(A, B))$. Now note that

$$C \equiv \left(\begin{array}{c|c} \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & C_1 \end{array}\right) \pmod{p^\gamma},$$

where C_1 is a 3×3 matrix with entries in $\mathbb{Z}_p$. Also

$$D \equiv \left(\begin{array}{c|c} \mathbf{0} & \mathbf{v^t} \\ \hline \mathbf{v} & D_1 \end{array}\right) \pmod{p^\gamma},$$

where D_1 is a 3×3 matrix with entries in $\mathbb{Z}_p$, and $\mathbf{v} \in \mathbb{Z}_p^3$. It is now easily seen that the coefficients of X^4 and X^3Y in $G(X, Y) = \det(XC - YD)$ are congruent to 0 modulo p^γ. By considering the formula for the discriminant of G in terms of its coefficients, we see that $p^\gamma \mid \partial(C, D)$. This completes the proof. ∎

5.2. *The archimedean case.* Let A, B be $n \times n$ symmetric matrices with entries in $\mathbb{Z}$. Suppose further that $F(X, Y) = \det(XA - YB)$ is non-zero and does not have any repeated roots. We want to determine the local solubility of

$$\mathcal{H} : \begin{cases} \mathbf{x}^t A \mathbf{x} = 0, \\ \mathbf{x}^t B \mathbf{x} = 0 \end{cases}$$

over $\mathbb{R}$. As $\det(XA - YB)$ is non-zero, by taking appropriate linear combinations of A and B (if necessary), we can assume that $\det A$ and $\det B$ are non-zero. Hence $F(\lambda) = \det(A - \lambda B)$ is a polynomial of degree n with distinct roots.

The following lemma of Swinnerton-Dyer allows us to get a better grip on the problem.

LEMMA 6 (Swinnerton-Dyer). *Let* f, g *be homogeneous real quadratic forms. Then the manifold* $f = g = 0$ *contains non-zero real points if and only if the quadratic form* $\lambda f - \mu g$ *is not definite for all real* λ, μ.

P r o o f. This is part of Lemma 1 of [24]. ∎

We are now ready for a simplification:

LEMMA 7. *Suppose that* $F(\lambda) = \det(A - \lambda B)$ *has a non-real root. Then* $\mathcal{H}$ *has a non-trivial solution over* $\mathbb{R}$.

P r o o f. This is standard (see for example [15, p. 263–264]). ∎

By Lemma 7, we may restrict our attention to the case where $F(X, Y) = \det(XA - YB)$ has n real roots. Hence by the next lemma, the two matrices A, B are simultaneously diagonalisable over $\mathbb{R}$. Naturally, it is much easier to ask if there is a definite linear combination of two matrices when they are diagonal.

LEMMA 8. *Suppose that* $\det A, \det B$ *are non-zero, and that* $\det(A - YB)$ *is a polynomial of degree* n, *which has* n *real roots,* $\lambda_1, \ldots, \lambda_n$ *say. Let* $\mathbf{x}_1, \ldots, \mathbf{x}_n$ *be non-trivial vectors in* $\mathbb{R}^n$ *such that*

$$(A - \lambda_i B)\mathbf{x}_i = \mathbf{0}. \tag{4}$$

Let $P = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$, *the* $n \times n$ *matrix with the* $\mathbf{x}_i$ *as its columns. Then* $P \in \mathrm{GL}_n(\mathbb{R})$ *and*

$$P^t AP = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix}, \quad P^t BP = \begin{pmatrix} \beta_1 & & \\ & \ddots & \\ & & \beta_n \end{pmatrix}, \tag{5}$$

where $\alpha_i = \lambda_i \mathbf{x}_i{}^t B\mathbf{x}_i$, $\beta_i = \mathbf{x}_i{}^t B\mathbf{x}_i$.

P r o o f. This is straightforward. ∎

LEMMA 9. *Under the hypotheses and notation of Lemma* 8, $\mathcal{H}$ *has a non-trivial real solution if and only if there do not exist real* λ^*, μ^* (*not both zero*) *such that the real numbers* $\mu^*\alpha_i - \lambda^*\beta_i$ *all have the same sign.*

P r o o f. This is immediate from Lemmas 6 and 8. ∎

From this we can then deduce

LEMMA 10. *Under the hypotheses and notation of Lemma* 8, $\mathcal{H}$ *has no non-trivial real solution if and only if there exists* λ_j, *one of the roots of* $F(\lambda) = \det(A - \lambda B)$, *such that* $A - \lambda_j B$ *is semi-definite.*

P r o o f. Suppose first that $\mathcal{H}$ has no non-trivial real solution. By Lemma 10 above, there exist real λ^*, μ^* such that $\mu^*\alpha_i - \lambda^*\beta_i$ all have the same sign. If $\mu^* = 0$ then we can replace it by a very small non-zero real number and still have all $\mu^*\alpha_i - \lambda^*\beta_i$ of the same sign. Hence, we will assume that $\mu \neq 0$. By dividing by μ^*, we see that there is a real λ^{**} such that $\alpha_i - \lambda^{**}\beta_i$ all have the same sign. Let λ_j be the root of $F(\lambda)$ which is closest to λ^{**}. We note that as we vary λ along the real line, none of the $\alpha_i - \lambda\beta_i$ change

sign until we cross a root of $\prod(\alpha_i - \lambda\beta_i) = F(\lambda)$. Since λ_j is the closest root of $F(\lambda)$ to λ^{**}, it follows that $\alpha_i - \lambda_j\beta_i$, $i \neq j$, all have the same sign and that, of course, $\alpha_j - \lambda_j\beta_j = 0$. Hence $A - \lambda_j B$ is semi-definite, as required.

Conversely, suppose that $A - \lambda_j B$ is semi-definite, where λ_j is a root of $F(\lambda)$. Write

$$A = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix}, \quad B = \begin{pmatrix} \beta_1 & & \\ & \ddots & \\ & & \beta_n \end{pmatrix} \tag{6}$$

as in Lemma 8. Recall that the α's and β's are all non-zero, since by assumption $\det A, \det B \neq 0$. Since $A - \lambda_j B$ is semi-definite, the $\alpha_i - \lambda_j\beta_i$ are all of the same sign except $\alpha_j - \lambda_j\beta_j = 0$. Note $\alpha_j - (\lambda_j + \varepsilon)\beta_j = -\varepsilon\beta_j$; hence, since $\beta_j \neq 0$, by choosing ε small enough and with appropriate sign, we will have all $\alpha_i - (\lambda_j + \varepsilon)\beta_i$ of the same sign. Hence $A - (\lambda_j + \varepsilon)B$ is definite and the lemma follows. ∎

THEOREM 11. *Under the notation and hypotheses of Lemma* 8, $\mathcal{H}$ *has a non-trivial solution in* $\mathbb{R}$ *if and only if, for each* λ_j, *the real numbers* $\alpha_i - \lambda_j\beta_i$ $(i \neq j)$ *do not all have the same sign.*

Proof. Immediate from Lemma 10. ∎

This allows us to test for the real solubility of $\mathcal{H}$.

6. A special case. In this section we consider the problem of determining the local solubility at non-archimedean primes of an intersection of two quadric surfaces. As before we assume that these two surfaces are given by two symmetric 4×4 matrices, A and B. Using the method of the previous section can be very inefficient in terms of computing time. However, in this section we show how one can find a faster method in the case where $\det(AX + BY)$ has a linear factor over $\mathbb{Q}_p$. We shall assume for convenience that $p \neq 2$. So for the rest of this section we assume that $\det(AX + BY)$ has a linear factor over $\mathbb{Q}_p$. Now by a linear change of variable, defined over $\mathbb{Q}_p$, and taking appropriate linear combinations of $Q_1(\mathbf{x})$ and $Q_2(\mathbf{x})$, we can assume that $Q_1(\mathbf{x}) = \mathbf{x}^t A\mathbf{x}$ contains no x_4 terms and $Q_2(\mathbf{x}) = \mathbf{x}^t B\mathbf{x}$ contains only one term involving x_4 and this is of the form x_4^2.

In this situation $Q_1(\mathbf{x})$ determines a curve of genus zero. By another change of variable defined over $\mathbb{Q}_p$we may assume that $Q_1(\mathbf{x})$ is of the form

$$aX^2 + bY^2 + cZ^2 = 0 \tag{7}$$

with $a, b, c \in \mathbb{Z}_p$, and $v(a) = v(b) = 0$ and $v(c) = 0$ or 1. If $v(c) = 1$, then $-ab^{-1}$ must be a square in $\mathbb{Z}_p$, otherwise (7) does not have a solution over $\mathbb{Q}_p$ and we may stop. So if $\alpha^2 = -ab^{-1}$ then $(1, \alpha, 0)$ is a non-trivial solution to (7), and we are finished. If $v(c) = 0$, then heuristically, for 50% of pairs

(x, y), $-c^{-1}(ax^2 + by^2)$ is a square in $\mathbb{Z}_p$. Thus we expect to find a solution to $Q_1(\mathbf{x}) = 0$ in $O(1)$ steps, if $Q_1(\mathbf{x})$ is soluble. If $Q_1(\mathbf{x})$ is not soluble then certainly its intersection with $Q_2(\mathbf{x}) = 0$ will not be either.

Given one solution to $Q_1(\mathbf{x}) = 0$ we can parametrise all others in the form

$$z_1 : z_2 : z_3 = q_1(X_1, X_2) : q_2(X_1, X_2) : q_3(X_1, X_2), \tag{8}$$

where $q_i(X_1, X_2)$ are binary quadratic forms which can be explicitly determined. Suppose that $z_i = \alpha q_i(X_1, X_2)$ for some $\alpha \in \mathbb{Q}_p^*$. Substituting this into $\mathbf{z}^t B\mathbf{z} = 0$ we obtain an equation of the form $x_4^2 = g(X_1, X_2)$, where $g(X_1, X_2)$ is a binary quartic form with coefficients in $\mathbb{Z}_p$.

So we are reduced to finding whether

$$Y^2 = g(X)$$

has any solutions in $\mathbb{Q}_p$ (including any at infinity), where $g(X) \in \mathbb{Z}_p[X]$ is of degree 4 and has non-zero discriminant. First we note that this curve has a pair of points at infinity if and only if the leading coefficient of g is a square in $\mathbb{Z}_p$.

There are standard algorithms to solve this problem in the literature, see for instance [11] and [1]. However these methods have polynomial time complexity in p. In this section we give an algorithm with probabilistic polynomial time complexity in $\log p$ based on root extraction in finite fields. The method is deterministic polynomial time in $\log p$ assuming the Generalised Riemann Hypothesis [9, pp. 31–34 and 37].

If f is a polynomial in $\mathbb{Z}_p[X]$, we write $\bar{f}$ for the image of f under the map $\mathbb{Z}_p[X] \to \mathbb{F}_p[X]$ induced by the natural map $\mathbb{Z}_p \to \mathbb{F}_p$. If $\deg f = 4$ but $\deg \bar{f} \le 3$ we shall say that $\bar{f}$ has a *root at infinity*; if $\deg \bar{f} \le 2$ we shall say that $\bar{f}$ has a *multiple root at infinity*. These conventions should be borne in mind in what follows. We shall make repeated use of the following lemma.

Lemma 12. *Suppose the curve*

$$C : aY^2 = f(X) \tag{9}$$

is given with $f(X) \in \mathbb{Z}_p[X]$, $a \in \mathbb{Z}_p$. *Let* $x_1, y_1 \in \mathbb{Z}_p$ *such that* $ay_1^2 \equiv f(x_1) \pmod p$. *Then there exist* $x, y \in \mathbb{Z}_p$ *with* $x \equiv x_1$, $y \equiv y_1 \pmod p$ *such that* $ay^2 = f(x)$ *except possibly when* $ay_1 \equiv f'(x_1) \equiv 0 \pmod p$.

Proof. The conclusion follows by applying Hensel's Lemma to the polynomial

$$G_1(X) = f(X) - ay_1^2$$

in the case $f'(x_1) \not\equiv 0 \pmod p$, and to the polynomial

$$G_2(Y) = aY^2 - f(x_1)$$

in the case $ay_1 \not\equiv 0 \pmod p$. ∎

COROLLARY 1. *Suppose* $f(X) \in \mathbb{Z}_p[X]$ *such that* $\bar{f} \not\equiv 0 \pmod{p}$, *and* $\deg \bar{f} \leq 4$. *Then* $pY^2 = f(X)$ *has a solution in* $\mathbb{Q}_p$ *if* $\bar{f}$ *has a root defined over* $\mathbb{F}_p$ *which is not a repeated root.*

Using the above lemma, and its corollary, we shall give an algorithm to determine in probabilistic polynomial time whether

$$Y^2 = f(X) \tag{10}$$

has a solution in $\mathbb{Q}_p$. Before giving the complete algorithm we deduce two lemmas from Lemma 12.

LEMMA 13. *Suppose that* $f(X) \in \mathbb{Z}_p[X]$ *is such that* $\deg f = 4$ *and* $\deg \bar{f} = 3$ *or* 4. *Suppose* $\bar{f}(X)$ *has no repeated factors. Then equation* (10) *has solutions over* $\mathbb{Q}_p$.

Proof. Under the hypotheses of the lemma, the equation $Y^2 = \bar{f}(X)$ is a curve of genus 1 defined over $\mathbb{F}_p$. It follows (see [8, p. 119]) that it has at least one point defined over $\mathbb{F}_p$. Again, since $\bar{f}$ does not have repeated factors, we can use Lemma 12, with $a = 1$, to show that this solution lifts to one defined over $\mathbb{Q}_p$. ∎

LEMMA 14. *Suppose* $f(X) \in \mathbb{Z}_p[X]$ *is such that* $1 \leq \deg \bar{f} \leq 4$. *Suppose that* $\bar{f} = \overline{g}^2\overline{h}$ *where* $\deg \overline{g} \geq 0$, $\deg \overline{h} \geq 1$ *and* $\overline{h}$ *is a square-free polynomial. Then equation* (10) *has solutions in* $\mathbb{Q}_p$.

Proof. The curve $Y^2 = \overline{h}(X)$ has genus 0, and hence has $p + 1$ points defined over $\mathbb{F}_p$. Of these at most 2 are at infinity. Further, there is at most 1 root of g. If this root is x_0 say, then there are at most 2 points on $Y^2 = \overline{h}(X)$ whose x-coordinate is x_0. Hence if $p \geq 5$ then $Y^2 = \overline{h}(X)$ has at least one point $(x_1, y_1) \in \mathbb{F}_p^2$ with $x_1 \not\equiv x_0$. Then the point $(x_1, y_1\overline{g}(x_1))$ lifts to a point on $Y^2 = f(X)$ by Lemma 12. For the case $p = 3$ the lemma can be established by a lengthy but straightforward case-by-case check which we omit. ∎

The following corollary easily follows from the above lemmas.

COROLLARY 2. *Suppose* $\bar{f} \not\equiv 0$. *If equation* (10) *has no points over* $\mathbb{Q}_p$ *then* $\bar{f} \equiv \alpha\overline{g}^2$ *where* $\overline{g}(X) \in \mathbb{F}_p[X]$ *and* $\alpha \in \mathbb{F}_p^* \backslash \mathbb{F}_p^{*2}$.

Proof. The only case that remains to be checked is that if $\bar{f} \not\equiv 0$ and $\bar{f} \equiv \overline{g}^2$ then (10) has a solution over $\mathbb{Q}_p$. For this it is sufficient to choose any x_0 such that $g(x_0) \not\equiv 0 \pmod{p}$, and then note that $(x_0, g(x_0))$ lifts by Lemma 12. ∎

Using these results the following algorithm is immediate.

ALGORITHM 1. Testing

$$Y^2 = f(X) \tag{11}$$

for solubility over $\mathbb{Q}_p$, where $f(X) \in \mathbb{Z}_p[X]$, $\deg f = 4$, and the discriminant of f is non-zero.

Step I

• If $\overline{f} \equiv 0 \pmod{p}$, then go to Step II.

• Check if $\overline{f} = \overline{a}\,\overline{g}^2$ for some $\overline{g} \in \mathbb{F}_p[X]$, and $\overline{a} \in \mathbb{F}_p$. If this is not the case, or if $\overline{a} \in \mathbb{F}_p^{*2}$ then we have local solubility by the above theorems and we can stop.

• Hence we can assume that $\overline{f} = \overline{a}\,\overline{g}^2$, and $\overline{a} \notin \mathbb{F}_p^{*2}$. So any solution $(X_0,\ Y_0) \in \mathbb{Z}_p^2$ to (11) must satisfy $Y_0 \equiv 0$ and $\overline{g}(X_0) \equiv 0$. Now $\overline{g}$ has at most two solutions $\overline{\varepsilon}_1, \overline{\varepsilon}_2 \pmod{p}$; if $\overline{g}$ has no solutions in $\mathbb{F}_p$ then (11) has no solutions in $\mathbb{Z}_p$ and we can stop.

• Hence

$$Y_0 = pY_1 \quad \text{and} \quad X_0 = pX_1 + \varepsilon_i$$

where $Y_1, X_1 \in \mathbb{Z}_p$. Choose $a \in \mathbb{Z}_p$ and $g \in \mathbb{Z}_p[X]$ such that the images of a and g under $\mathbb{Z}_p \to \mathbb{F}_p$ are $\overline{a}$ and $\overline{g}$. Then $f = ag^2 + ph$ where h has coefficients in $\mathbb{Z}_p$. Since $p^2 \mid Y_0^2 = f(X_0)$ and $p \mid g(X_0)$, we find that $p \mid h(X_0)$. Hence if neither of ε_1 and ε_2 is a root of $\overline{h}$ then (11) is not soluble and we can stop.

• If say ε_i is a root of $\overline{h}$ then p divides the trailing coefficient of $h(pX+\varepsilon_i)$. So we will get at most 2 equations of the form

$$Y^2 = f_i(X)$$

where $f_i(X) = \frac{1}{p^2} f(pX + \varepsilon_i) \in \mathbb{Z}_p[X]$. It is now necessary and sufficient that one of these should have solutions in $\mathbb{Z}_p$, and we use Step I again with f_i instead of f.

Step II

• Here f is divisible by p. If f is divisible by p^2 then we can replace f by $\frac{1}{p^2} f$ and go to Step I.

• So suppose that $f_1 = \frac{1}{p} f \not\equiv 0 \pmod{p}$. We see that we want to determine if

$$pY_1^2 = f_1(X)$$

has solutions in $\mathbb{Z}_p$. If f_1 has no roots in $\mathbb{F}_p$ then (11) is not soluble and we can stop.

• If f_1 has a root which is not a repeated root then (11) is soluble and we can stop.

• Suppose that f_1 has repeated roots ε_i where $i = 1$, or $i = 1, 2$. Then it is necessary and sufficient to determine if either of

$$Y_1^2 = \frac{1}{p} f_1(pX_1 + \varepsilon_i)$$

is soluble, and $\frac{1}{p} f_1(pX_1 + \varepsilon_i) \in \mathbb{Z}_p[X]$. So we use Step I again.

LEMMA 15. *Suppose $r = v(\partial g)$ where ∂g is the discriminant of g. In the above algorithm, if we are still undecided after $r+1$ steps, then the equation* (11) *has a solution defined over $\mathbb{Q}_p$ and we can stop.*

Proof. It is clear that after r steps, we may write down a $Z \in \mathbb{Z}_p$ such that $f(Z) \equiv 0 \pmod{p^{2(r+1)}}$. By [7, p. 52], f has a root in $\mathbb{Z}_p$. This immediately implies that (11) has a solution defined over $\mathbb{Q}_p$. ∎

7. Examples. We give an example which shows how you can prove the 2-primary part of the Tate–Shafarevich group is a given number. We look at the curve

$$Y^2 + Y = X^3 - X^2 - 929X - 10595.$$

This has conductor 571, and conjectured rank equal to 0 with no two torsion. The Birch–Swinnerton-Dyer conjectures imply that the Tate–Shafarevich group has order 4.

Applying **mwrank** we find that the three rogue homogeneous spaces in the 2-Selmer group are given by

$$\begin{aligned} Y^2 &= -229X^4 - 135X^3 - 238X^2 - 84X - 8, \\ Y^2 &= -108X^4 - 4X^3 - 76X^2 - 112X - 31, \\ Y^2 &= -4X^4 + 4X^3 + 92X^2 - 104X - 727. \end{aligned}$$

Note if you start with an elliptic curve with no two-torsion then the first descents will always involve irreducible quartics.

The first of these is isomorphic to

$$-229y^2 = x^4 - 135x^3z + 54502x^2z^2 - 4405044xz^3 + 96071912z^4.$$

Working in the field $\mathbb{Q}(\theta)$, where $\theta^4 - 2\theta^3 + 2\theta^2 - 4\theta - 1 = 0$, we find that there are 8 possible descendants. All of these are, however, insoluble over $\mathbb{Q}_{571}$.

Similarly the second equation is isomorphic to

$$-3y^2 = x^4 - 4x^3 + 8208x^2 - 1306368x + 39051072.$$

Working in the field $\mathbb{Q}(\phi)$ where $\phi^4 - 2\phi^2 - 2\phi - 3 = 0$, we find that there are at most 8 descendants. Again we find that they are all insoluble over $\mathbb{Q}_{571}$.

The last equation is isomorphic to

$$-y^2 = x^4 + 4x^3 - 368x^2 - 1664x + 46528,$$

and working in the relevant quartic number field we immediately see (by the norm condition) that this has no descendants and hence has no rational points. Hence the Tate–Shafarevich group has 2 primary part of order 4.

References

[1] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. Reine Angew. Math. 212 (1963), 7–25.

[2] —, —, *Notes on elliptic curves. II*, ibid. 218 (1965), 79–108.

[3] A. Bremner, *On the equation* $y^2 = x(x^2+p)$, in: Number Theory and Applications, R. A. Mollin (ed.), Kluwer, Dordrecht, 1989, 3–23.

[4] A. Bremner and J. W. S. Cassels, *On the equation* $y^2 = x(x^2+p)$, Math. Comp. 42 (1984), 257–264.

[5] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. 41 (1966), 193–291.

[6] —, *The Mordell–Weil group of curves of genus 2*, in: Arithmetic and Geometry Papers Dedicated to I. R. Shafarevich on the Occasion of his Sixtieth Birthday, Vol. 1, Birkhäuser, 1983, 29–60.

[7] —, *Local Fields*, London Math. Soc. Student Texts, Cambridge University Press, 1986.

[8] —, *Lectures on Elliptic Curves*, London Math. Soc. Student Texts, Cambridge University Press, 1991.

[9] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, Berlin, 1993.

[10] I. Connell, *Addendum to a paper of Harada and Lang*, J. Algebra 145 (1992), 463–467.

[11] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.

[12] J. Gebel, A. Pethő and H. G. Zimmer, *Computing integral points on elliptic curves*, Acta. Arith. 68 (1994), 171–192.

[13] J. Gebel and H. G. Zimmer, *Computing the Mordell–Weil group of an elliptic curve over* $\mathbb{Q}$, in: Elliptic Curves and Related Topics, H. Kisilevsky and M. Ram Murty (eds.), CRM Proc. Lecture Notes 4, Amer. Math. Soc., 1994.

[14] M. J. Greenberg, *Lectures on Forms in Many Variables*, W. A. Benjamin, 1969.

[15] W. H. Greub, *Linear Algebra*, Springer, 1967.

[16] M. J. Razar, *A relation between the two component of the Tate–Šafarevič group and* $L(1)$ *for certain elliptic curves*, Amer. J. Math. 96 (1974), 127–144.

[17] S. Siksek, *Descents on Curves of Genus* 1, PhD thesis, Exeter University, 1995.

[18] —, *Infinite descent on elliptic curves*, Rocky Mountain J. Math. 25 (1995), 1501–1538.

[19] S. Siksek and N. P. Smart, *On the complexity of computing the* 2*-Selmer group of an elliptic curve*, preprint, 1995.

[20] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.

[21] N. P. Smart, *S-integral points on elliptic curves*, Proc. Cambridge Philos. Soc. 116 (1994), 391–399.

[22] N. P. Smart and N. M. Stephens, *Integral points on elliptic curves over number fields*, ibid., to appear, 1996.
[23] R. J. Stroeker and N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta. Arith. 67 (1994), 177–196.
[24] H. P. F. Swinnerton-Dyer, *Rational zeros of two quadratic forms*, ibid. 9 (1964), 261–270.
[25] J. A. Todd, *Projective and Analytical Geometry*, Pitman, 1947.
[26] A. Weil, *Number Theory. An Approach Through History*, Birkhäuser, 1984.

Institute of Mathematics and Statistics
University of Kent at Canterbury
Canterbury, Kent, England
E-mail: J.R.Merriman@ukc.ac.uk
S.Siksek@ukc.ac.uk
N.P.Smart@ukc.ac.uk

Received on 5.3.1996 (2939)