ACTA ARITHMETICA
179.1 (2017)

On representing coordinates of points on elliptic curves by quadratic forms

by

Andrew Bremner (Tempe, AZ) and Maciej Ulas (Kraków)

1. Introduction. Cornelissen and Zahidi [3] introduce the quartic surface defined by the equation

$$V:\ (A^2+B^2)(A^2+11B^2)=225(P^2-5Q^2)^2, \tag{1}$$

with interest in the rational points on V in regard to undecidability questions in mathematical logic. There is an associated elliptic curve

$$E:\ Y^2=(X^2+1)(X^2+11),$$

and the existence of rational points on V is equivalent to the existence of rational points on E whose Y-coordinate is representable by the quadratic form $15(P^2-5Q^2)$. The curve E has rational rank 1, with generator $(1/2, 15/4)$, so the group $E(\mathbb{Q})$ is explicitly known. But the problem of deciding whether the Y-coordinate of a point can be represented by the form $15(P^2-5Q^2)$ demands knowledge of the factorization of the Y-coordinate into primes, which becomes computationally intractable for a point given by a large multiple of the generator.

Here, we investigate the question of when the Y-coordinate of a rational point on an elliptic quartic can be represented by a quadratic form, and in particular give several examples of equations of surfaces of type

$$\mathcal{V}:\ c_0+c_1x+c_2x^2+c_3x^3+c_4x^4=(ap^2+bq^2)^2, \qquad a,b,c_i\in\mathbb{Q},$$

where we can deduce the existence of infinitely many rational points. This is achieved by constructing a hyperelliptic quartic curve $\mathcal{C}'$ with a map $\psi:\mathcal{C}'\to\mathcal{V}$. When $\mathcal{C}'$ is an elliptic curve of positive rank, the result will follow.

2010 *Mathematics Subject Classification*: 11D25, 11D41, 11E16, 11G05.
Key words and phrases: Diophantine equations, rational points, elliptic curves, representations, quadratic forms.
Received 29 August 2016.
Published online 19 May 2017.

DOI: 10.4064/aa8597-1-2017

Second, we consider elliptic curves $E : Y^2 = f(X)$, f cubic, and use similar techniques to investigate when there can be infinitely many rational points on E with X-coordinate representable by a quadratic form $ap^2 + bq^2$. We illustrate the ideas with many examples. Throughout the paper, an important role is played by the use of machine computations, particularly using the computer algebra system Magma [1].

2. First construction. Let $a, b \in \mathbb{Z}$, where we suppose that the quadratic form $ax_1^2 + bx_2^2$ is irreducible, and let $f(X) = \sum_{i=0}^{4} c_i X^i \in \mathbb{Q}[x]$ be a non-singular quartic. We are interested in when the quartic curve

$$\mathcal{C}:\ Y^2 = f(X)$$

can have infinitely many rational points with the Y-coordinate being representable by the quadratic form $ax_1^2 + bx_2^2$. Consider the quartic surface given by the equation

$$\mathcal{V}:\ (ap^2 + bq^2)^2 = f(X).$$

Multiplying through by a^2, we may suppose without loss of generality that $a = 1$. Suppose $(p_0, q_0, X_0) \in \mathcal{V}(\mathbb{Q})$. Then $f(X_0) \neq 0$, otherwise $p_0^2 + bq_0^2 = 0$ and the form $p^2 + bq^2$ is reducible. It is clear that there exist infinitely many points $(p, q, X_0) \in \mathcal{V}(\mathbb{Q})$, because the conic $p_0^2 + bq_0^2 = p^2 + bq^2$ is rationally parametrizable. Further, from this observation and the fact that the curve $p^4 = f(X)$ is of genus 3, it is also clear that we may assume if necessary that $p_0 q_0 \neq 0$. When we refer to $\mathcal{V}(\mathbb{Q})$ being infinite, we shall henceforth mean that $\pi_X(\mathcal{V}(\mathbb{Q}))$ is infinite, where $\pi_X : \mathcal{V}(\mathbb{Q}) \to \mathbb{Q}$ is the projection onto the X-coordinate. It is clear that a necessary condition for $\mathcal{V}$ to have infinitely many rational points is that the set $\mathcal{C}(\mathbb{Q})$ is infinite.

Following a suitable change of variable we can move the point (p_0, q_0, X_0) to infinity and eliminate the coefficient of X^3 in f. We thus consider the quartic surface

$$\mathcal{V}:\ (p^2 + bq^2)^2 = m^2X^4 + a_2X^2 + a_1X + a_0, \qquad m = p_0^2 + bq_0^2.$$

In order to find more points on $\mathcal{V}$, write

$$(2) \qquad p = p_0T, \quad q = q_0T + U/p_0, \qquad X = T + V,$$

where U, V, T are to be determined. This substitution gives

$$(p^2 + bq^2)^2 - f(X) = \sum_{i=0}^{3} C_i T^i,$$

where $C_i \in \mathbb{Q}[U, V]$ for $i = 0, 1, 2, 3$. In particular $C_3 = -4m(mp_0V - bq_0U)/p_0$. Taking $V = bq_0U/mp_0$, we obtain $F(T) := B_2T^2 + B_1T + B_0 = 0$ where $B_i = B_i(U)$ is in general of degree $4 - i$ for $i = 0, 1, 2$. Now a point of the form (2) lies on $\mathcal{V}$ if and only if $F(T) = 0$ has rational roots, which is equivalent to the existence of $U \in \mathbb{Q}$ such that the discriminant of F with respect to T is a square in $\mathbb{Q}$. We thus consider the curve $\mathcal{C}' : W^2/m^2 = B_1^2 - 4B_0B_2$, that is,

$$\mathcal{C}' :\ W^2 = -8b^3U^6 + 4b^2a_2U^4 + 8ba_0m^2U^2 + (a_1^2 - 4a_0a_2)m^2 =: G(U).$$

Here, $T = (-B_1 + W/m)/(2B_2)$. For general coefficients a_0, a_1, a_2 and given b the curve $\mathcal{C}'$ is hyperelliptic of genus 2. By the Faltings Theorem, the set $\mathcal{C}'(\mathbb{Q})$ is finite. Thus a necessary condition for $\mathcal{C}'$ to have infinitely many rational points is the vanishing of the discriminant (with respect to U) of the polynomial G. In this case the genus of $\mathcal{C}'$ is at most 1 and there is a chance for $\mathcal{C}'$ to have infinitely many rational points.

Remark 2.1. If the approach of this section is used on the surface (1), then the corresponding curve $\mathcal{C}'$ is of genus 2.

We have

$$\mathrm{Disc}_U(G) = 2^{21}b^{15}(a_1^2 - 4a_0a_2)m^2\,\mathrm{Disc}_X(f(X))^2,$$

and since $\mathrm{Disc}_X(f(X)) \neq 0$, it follows that $\mathrm{Disc}_U(G) = 0$ if and only if $a_1^2 - 4a_0a_2 = 0$. Hence the polynomial f takes the form

$$f(X) = m^2X^4 + c(dX + e)^2$$

for some $c, d, e \in \mathbb{Q}$ with $ce \neq 0$. If $d \neq 0$ then we can clearly assume that $d = 1$. The corresponding polynomial G is divisible by $4U^2$ and the curve $\mathcal{C}'$ may now be taken in the form

$$\mathcal{C}' :\ w^2 = -b(2b^2U^4 - bcd^2U^2 - 2ce^2m^2),$$

with $W = 2Uw$.

Tracing back the maps, we obtain the mapping

$$\psi : \mathcal{C}' \ni (U, w) \mapsto (p, q, X) \in \mathcal{V}$$

given by

$$\begin{aligned} p &= \frac{p_0cdem - bq_0U(2bU^2 - cd^2) + p_0Uw}{m(2bU^2 - cd^2)}, \\ q &= \frac{cdeq_0m + p_0U(2bU^2 - cd^2) + q_0Uw}{m(2bU^2 - cd^2)}, \\ X &= \frac{cdem + Uw}{m(2bU^2 - cd^2)}. \end{aligned} \tag{3}$$

The following theorem now follows:

Theorem 2.2. *Let $\mathcal{V}$ denote the surface $(p^2+bq^2)^2 = m^2X^4+c(dX+e)^2$, and let $\mathcal{C}'$ be the quartic curve $w^2 = -b(2b^2U^4 - bcd^2U^2 - 2ce^2m^2)$. Then $\mathcal{C}'(\mathbb{Q})$ infinite implies $\mathcal{V}(\mathbb{Q})$ infinite.*

Proof. Assume that the set $\mathcal{C}'(\mathbb{Q})$ is infinite. To get the result it is enough to prove that the image of the map ψ constructed above is infinite in the set $\mathcal{V}(\mathbb{Q})$. This is equivalent to the fact that if $(p',q',X')\in\mathcal{V}(\mathbb{Q})$ and $Y=p'^2+bq'^2$ then there are only finitely many rational points $(U,w)\in\mathcal{C}'$ such that $p^2+bq^2=Y$, where p,q are given by (3). Eliminating w between the equations

$$Y=p^2+bq^2,\qquad w^2=-b(2b^2U^4-bcd^2U^2-2ce^2m^2)$$

gives an equation of degree 12 in U, which is not identically zero since the coefficient of U^{12} equals $4b^6p_0^4(-1+2p_0^4)^2(p_0^2+bq_0^2)^2$. Hence there are only finitely many possibilities for U, as required. ■

Remark 2.3. It has been pointed out to us that $\mathcal{C}'(\mathbb{Q})$ infinite in the hypothesis of the theorem may be weakened to $\mathcal{C}'(\mathbb{Q})\neq\emptyset$ and $\mathcal{C}(\mathbb{Q})$ infinite. For if E' denotes the elliptic curve associated to $\mathcal{C}'$, then the composition $\varphi:\mathcal{C}'\to\mathcal{V}\to\mathcal{C}$ extends to a finite morphism $E'\to E$. If $\mathcal{C}'(\mathbb{Q})\neq\emptyset$, take a rational point in $\mathcal{C}'(\mathbb{Q})$, corresponding to $O'\in E'(\mathbb{Q})$, and let its image under φ correspond to $O\in E(\mathbb{Q})$. Then φ induces an isogeny $(E',O')\to(E,O)$ of degree 2. Thus if $\mathcal{C}(\mathbb{Q})$ is infinite, then either $\mathcal{C}'(\mathbb{Q})$ is empty or $\mathcal{C}'(\mathbb{Q})$ is infinite.

It is straightforward to compute a cubic model E for $\mathcal{C}$; E takes the form

$$E:\ y^2=x(x^2+cd^2x-4ce^2m^2),$$

with the map $\mathcal{C}\to E$ given by

$$(x,y)=\big(-2m(Y-mX^2),\ -2m(2m^2X^3-2mXY+cd^2X+cde)\big).$$

The curve $\mathcal{C}'$ occurs as a homogeneous space in a standard 2-descent on E, on setting x equal either to $-2b$ or $2bc$ in $\mathbb{Q}^*/\mathbb{Q}^{*2}$. It follows that $\mathcal{C}'(\mathbb{Q})\neq\emptyset$ provided that there exists a point $(X_0,Y_0)\in\mathcal{C}(\mathbb{Q})$ with $Y_0-X_0^2\equiv b\delta \bmod \mathbb{Q}^{*2}$, where $\delta=m$ or $-mc$.

Example 2.4. Let $(p_0,q_0)=(1,0)$ and $(b,c,d,e)=(1,\ell,0,1)$ where ℓ is prime, so that $\mathcal{C}:Y^2=X^4+\ell$ and $\mathcal{C}':w^2=2(\ell-U^4)$. Assume the rank of $\mathcal{C}$ is positive, with (X_0,Y_0) a point of infinite order. Without loss of generality, on changing the sign of Y_0 if necessary, $Y_0-X_0^2=\alpha^2$ and $Y_0+X_0^2=\ell/\alpha^2$. Then $(U,w)=(\alpha,2\alpha X_0)$ is a point on $\mathcal{C}'$ of infinite order. Accordingly, the set of rational points on the surface

$$\mathcal{V}:\ (p^2+q^2)^2=X^4+\ell$$

is infinite. The above mapping reduces to

$$(U,w)\mapsto(p,q,X)=\left(\frac{w}{2U},U,\frac{w}{2U}\right).$$

Example 2.5. Set $D=m^2(m^2+2n^2)$ with $P=(n,m^2+n^2)$ a point of infinite order on the curve $\mathcal{C}:Y^2=X^4+D$. Take $b=1$, so that $\mathcal{C}'$:

$w^2 = 2(D - U^4)$ with $P' = (m, 2mn)$ a point of infinite order. Then the set of rational points on the surface

$$\mathcal{V}:\ (p^2 + q^2)^2 = X^4 + D$$

is infinite.

3. Quartics of type $X^4 + a_2X^2 + a_0$. In this section we are interested in rational points (X, Y) lying on the quartic curve

$$\mathcal{C}:\ Y^2 = X^4 + a_2X^2 + a_0,$$

with Y representable by the quadratic form $p^2 + bq^2$. Before stating any result, we observe that if the set $\mathcal{C}(\mathbb{Q})$ is infinite then there are infinitely many rational points in $\mathcal{C}(\mathbb{Q})$ with Y-coordinate represented by the quadratic form $p^2 - (a_2^2 - 4a_0)q^2$. Indeed, this is a consequence of the addition law on $\mathcal{C}$ which says that if $P_i = [i]P_1 = (X_i, Y_i) = (U_i/W_i, V_i/W_i^2)$, where $P_1 = (X_1, Y_1)$ is a point on $\mathcal{C}$ of infinite order, then

$$\begin{aligned} U_{2i} &= U_i^4 - a_0W_i^4, & U_{2i+1}U_1 &= U_i^2U_{i+1}^2 - a_0W_i^2W_{i+1}^2,\\ V_{2i} &= V_i^4 - (a_2^2 - 4a_0)U_i^2W_i^2, & W_{2i+1}W_1 &= U_i^2W_{i+1}^2 - U_{i+1}^2W_i^2,\\ W_{2i} &= 2U_iV_iW_i, & V_{2i+1}V_1 &= V_i^2V_{i+1}^2 - (a_2^2 - 4a_0)U_i^2U_{i+1}^2W_i^2W_{i+1}^2, \end{aligned}$$

for $i \in \mathbb{N}$ (see [2]). We thus see that the Y-coordinate of the point P_{2i} is representable by the form $p^2 - (a_2^2 - 4a_0)q^2$. The same property holds for the point P_{2i+1} provided that Y_1 is also so representable.

Remark 3.1. These formulas show the restrictive nature of the method presented in the previous section. Indeed, if we consider the surface $\mathcal{V}$: $(p^2 + 3q^2)^2 = X^4 + 3$ then the method of the previous section fails, since the corresponding quartic $\mathcal{C}' : w^2 = -3(18U^4 - 6)$ is not locally solvable at 2, and thus has no rational points. However, for $f(X) = X^4 + 3$ we have $a_0 = 3$, $a_2 = 0$, $a_2^2 - 4a_0 = -12$ and the above formulas show that the set of rational points on the surface $\mathcal{V}$ is infinite. (In order to prove this, it is enough to start with the point $P_1 = (U_1/W_1, V_1/W_1^2) = (1, 2)$ and compute the even multiples.)

In light of this remark, and the above formulas, the question arises as to whether Y-coordinates of rational points on C may be represented by other forms of type $p^2 + bq^2$ with $b \neq -(a_2^2 - 4a_0)$. We suppose

$$\mathcal{V}:\ (p^2 + bq^2)^2 = H(X) = X^4 + a_2X^2 + a_0, \quad a_0(a_2^2 - 4a_0) \neq 0,$$

and assume the existence of a (finite) point $(p, q, X) = (p_0, q_0, r_0)$, $r_0 \neq 0$, which implies

$$a_0 = m^2 - r_0^4 - a_2r_0^2, \quad m = p_0^2 + bq_0^2.$$

Set

$$p = p_0 + T, \quad q = q_0 + uT, \quad X = r_0 + vT.$$

This leads to a quartic polynomial in T with constant term 0. We make the coefficient of T equal to 0 by taking

$$v = \frac{2m(p_0 + bq_0u)}{r_0(a_2 + 2r_0^2)}.$$

We now have $C_2(u)T^2 + C_3(u)T^3 + C_4(u)T^4 = 0$. The discriminant $C_3(u)^2 - 4C_2(u)C_4(u)$ must be square for rational T, so gives an equation

$$-8mr_0^2(a_2 + 2r_0^2)F_2(u)F_4(u) = \square, \tag{4}$$

where $F_2(u)$, $F_4(u)$ are polynomials of degree 2, 4 respectively. If this sextic curve is to have genus at most 1, the discriminant with respect to u of $F_2(u)F_4(u)$ must vanish. The factorization is

$$2^{56}a_0^2b^{15}m^{34}r_0^{50}(a_2 + 2r_0^2)^{31}(a_2^2 - 4a_0)^4(2a_0 + a_2r_0^2) \\ \times (16a_0^3 + 32a_0^2a_2r_0^2 + 16a_0^2r_0^4 + 24a_0a_2^2r_0^4 - a_2^4r_0^4 + 32a_0a_2r_0^6 + 16a_0r_0^8),$$

and so the following three distinct possibilities arise.

- If the factor $2a_0 + a_2r_0^2$ vanishes, then

$$(a_2, a_0) = \big(2(m^2 - r_0^4)/r_0^2, -(m^2 - r_0^4)\big),$$

and the sextic (4) becomes

$$-2b(-q_0 + p_0u)^2L_4(u) = \square,$$

with $L_4(u)$ quartic in u:

$$L_4(u) = (m^4 - p_0^2(m + bq_0^2)r_0^4) - 4b^2p_0q_0^3r_0^4u + 2b(m^4 - (m^2 - 3bp_0^2q_0^2)r_0^4)u^2 \\ - 4b^2p_0^3q_0r_0^4u^3 + b^2(m^4 - b(m + p_0^2)q_0^2r_0^4)u^4.$$

The discriminant of $L_4(u)$ is $-2^8b^6m^{14}r_0^8a_0^3$, so is non-zero. It follows that there exists a non-constant rational map $\psi_1 : \mathcal{C}_1 \to \mathcal{V}_1$ where $\mathcal{C}_1$ is the genus 1 curve given by

$$\mathcal{C}_1 :\ -2bL_4(u) = \square \tag{5}$$

and $\mathcal{V}_1$ corresponds to our choice of a_0, a_2.

Example 3.2. Take $b = 3$ and $(p_0, q_0, r_0) = (1, 0, 2)$. Then $(a_2, a_0) = (-15/2, 15)$ and we have a mapping $\psi_1 : \mathcal{C}_1 \to \mathcal{V}_1$ where

$$\mathcal{C}_1 :\ V^2 = 2(5 + 30u^2 - 3u^4), \qquad \mathcal{V}_1 :\ (p^2 + 3q^2)^2 = X^4 - \tfrac{15}{2}X^2 + 15$$

given by

$$(p, q, X) \\ = \left(\frac{(5 + 3u^4 - uV)}{(-1 + u^2)(5 + 3u^2)}, -\frac{u(-10 + 2u^2 + uV)}{(-1 + u^2)(5 + 3u^2)}, \frac{2(5 + 3u^4 - uV)}{(-1 + u^2)(5 + 3u^2)}\right).$$

Since $\mathcal{C}_1$ is elliptic of rational rank 2, with generators $(-1,8)$, $(-3,8)$, it follows that there are infinitely many rational points on the elliptic curve

$$Y^2 = X^4 - \tfrac{15}{2}X^2 + 15$$

whose Y-coordinate can be represented by the quadratic form p^2+3q^2. We note that the curve $\mathcal{C}_1$ is 2-isogenous to the curve corresponding to $\mathcal{V}_1$.

- If the factor $a_2 + 2r_0^2$ vanishes, then

$$(a_2, a_0) = (-2r_0^2, m^2 + r_0^4),$$

and we have to eliminate u rather than v. This gives a quartic equation of the form

$$\text{(6)} \qquad \mathcal{C}_2:\ 2b(-m^2 + 2bq_0^2r_0^2v^2 + b^2q_0^4v^4) = \square;$$

the discriminant of the quartic is $-2^{14}b^{12}m^2q_0^{12}(m^2+r_0^4)^2$, and hence non-zero, so that $\mathcal{C}_2$ is of genus 1. Accordingly we have a non-constant rational map $\psi_2 : \mathcal{C}_2 \to \mathcal{V}_2$, where $\mathcal{V}_2$ corresponds to our choice of a_0, a_2.

Example 3.3. Take $b=2$ and $(p_0,q_0,r_0)=(1,1,1)$. Then $(a_2,a_0) = (-2,10)$ and we have a mapping $\psi_2 : \mathcal{C}_2 \to \mathcal{V}_2$ where

$$\mathcal{C}_2:\ U^2 = -9 + 4v^2 + 4v^4, \qquad \mathcal{V}_2:\ (p^2+2q^2)^2 = X^4 - 2X^2 + 10$$

given by

$$(p,q,X) = \left(\frac{9+8v^3-4v^4-6U}{9-4v^4}, \frac{9-4v^3-4v^4+3U}{9-4v^4}, \frac{9+4v^4-6Uv}{9-4v^4}\right).$$

Since $\mathcal{C}_2$ is of rational rank 1, with generator $(3/2, 9/2)$, it follows that there are infinitely many rational points on the elliptic curve

$$Y^2 = X^4 - 2X^2 + 10$$

whose Y-coordinate can be represented by the quadratic form p^2+2q^2. Moreover, one can check that the curve $\mathcal{C}_2$ is 2-isogenous to the curve corresponding to $\mathcal{V}_2$.

- The last factor in the discriminant defines a quartic curve in a_0, a_2 of genus 0 over $\mathbb{Q}(r_0)$. A parametrization is given by

$$(a_2, a_0) = \left(\frac{2t(r_0^2 + r_0t + t^2)}{r_0}, t^4\right).$$

The condition that (p_0,q_0,r_0) be a solution becomes

$$(p_0^2 + bq_0^2)^2 = (r_0+t)^2(r_0^2+t^2),$$

so that necessarily $r_0^2 + t^2 = \square$. Set $t = r_0(s^2-1)/(2s)$, where $s \neq 0, \pm 1$. Then

$$(a_2, a_0) = \left(\frac{r_0^2(s^2-1)(s^4+2s^3+2s^2-2s+1)}{4s^3}, r_0^4\frac{(s^2-1)^4}{16s^4}\right),$$

$$p_0^2 + bq_0^2 = \frac{(s^2+1)(s^2+2s-1)}{4s^2} r_0^2.$$

The quartic $H(X)$ now takes the form

$$\frac{1}{16s^4}\big(r_0^2(s+1)^3(s-1)+4sX^2\big)\big(r_0^2(s+1)(s-1)^3+4s^3X^2\big);$$

that is,

$$\mathcal{V}:\ 16s^4(p^2+bq^2)^2 = \big(r_0^2(s+1)^3(s-1)+4sX^2\big)\big(r_0^2(s+1)(s-1)^3+4s^3X^2\big),$$

where we demand a solution (p_0, q_0, r_0) of

$$p_0^2 + bq_0^2 = \frac{(s^2+1)(s^2+2s-1)}{4s^2} r_0^2. \tag{7}$$

The sextic (4) has become

$$-bs(-q_0+p_0u)^2 g_1(u) g_2(u) = \square, \tag{8}$$

where

$$g_1(u) = \big((1-s^2)p_0^2+2sbq_0^2\big)+2(1-2s-s^2)bp_0q_0u+b\big(2sp_0^2+(1-s^2)bq_0^2\big)u^2,$$
$$g_2(u) = 2(1-s^2)^2p_0^2+(1+s^2)^2bq_0^2+2(1-6s^2+s^4)bp_0q_0u$$
$$+ b((1+s^2)^2p_0^2+2(1-s^2)^2bq_0^2)u^2.$$

The discriminants of g_1, g_2 cannot vanish, and g_1, g_2 have no common root. Accordingly, there is a non-constant rational map $\psi_3 : \mathcal{C}_3 \to \mathcal{V}_3$, where $\mathcal{C}_3$ is the genus 1 curve

$$\mathcal{C}_3:\ -bsg_1(u)g_2(u) = \square \tag{9}$$

and $\mathcal{V}_3$ corresponds to our choice of a_0, a_2.

Example 3.4. Take $b=-5$ and $s=1/2$. The conic (7) is $p_0^2-5q_0^2 = \frac{5}{16}r_0^2$ with point $(p_0, q_0, r_0) = (5/8, 1/8, 1)$. Then $(a_2, a_0) = (-39/32, 81/256)$, and

$$\mathcal{V}_3:\ (p^2-5q^2)^2 = X^4 - \tfrac{39}{32}X^2 + \tfrac{81}{256}.$$

The associated elliptic quartic at (9) above is now

$$\mathcal{C}_3:\ 2(-11-10u+85u^2)(-13-14u+107u^2) = \square,$$

with a point at $u=-1/3$, and cubic model

$$y^2 = x^3 + 588x^2 + 36x \tag{10}$$

of rank 1 with generator $(36, -900)$. On replacing X by $1/8X$, it follows that there are infinitely many rational points on the elliptic curve

$$Y^2 = X^4 - 78X^2 + 1296 = (X^2-24)(X^2-54)$$

whose Y-coordinate can be represented by the quadratic form p^2-5q^2. As in the previous examples, one can check that the curve $\mathcal{C}_3$ is 2-isogenous to the curve corresponding to $\mathcal{V}_3$.

EXAMPLE 3.5. Take $b = -17$ and $s = 5$. The conic (7) is $p_0^2 - 17q_0^2 = \frac{221}{25} r_0^2$, with point $(p_0, q_0, r_0) = (-119/40, -1/40, 1)$. But the u-quartic at (9) is

$$y^2 = 102(10001 - 4046u + 71009u^2)(-239735 + 28322u + 2388313u^2),$$

which is locally unsolvable at 17. The X-quartic here is

$$Y^2 = H(X) = X^4 + \tfrac{5496}{125} X^2 + \tfrac{20736}{625},$$

which has cubic model $y^2 = x^3 + 12270x^2 + 31212000x$ of rank 1. So the X-quartic has rank 1, but the u-quartic has no points. The Jacobian of the u-quartic *is* 2-isogenous to the X-quartic.

Using exactly the same type of reasoning as in the proof of Theorem 2.2 one can prove that for each $i \in \{1, 2, 3\}$ the image of the map $\psi_i : \mathcal{C}_i \to \mathcal{V}_i$ is not finite provided that $\mathcal{C}_i(\mathbb{Q})$ is infinite. We omit these details and summarize our results in the following:

THEOREM 3.6. *Let $m = p_0^2 + bq_0^2$. Suppose the set of rational points on the curve*

$$\begin{aligned}\mathcal{C}_1 :\ -2b\big((m^4 - p_0^2(m + bq_0^2)r_0^4) - 4b^2 p_0 q_0^3 r_0^4 u + 2b(m^4 - (m^2 - 3bp_0^2 q_0^2) r_0^4) u^2 \\ - 4b^2 p_0^3 q_0 r_0^4 u^3 + b^2(m^4 - bq_0^2(m + p_0^2) r_0^4) u^4\big) = \square\end{aligned}$$

is infinite. Then the set of rational points on the surface

$$V_1 :\ (p^2 + bq^2)^2 = X^4 + \frac{2(m^2 - r_0^4)}{r_0^2} X^2 - (m^2 - r_0^4)$$

is infinite too (with the convention at the head of Section 2).

THEOREM 3.7. *Let $m = p_0^2 + bq_0^2$. Suppose the set of rational points on the curve*

$$\mathcal{C}_2 :\ 2b(-m^2 + 2bq_0^2 r_0^2 v^2 + b^2 q_0^4 v^4) = \square$$

is infinite. Then the set of rational points on the surface

$$V_2 :\ (p^2 + bq^2)^2 = X^4 - 2r_0^2 X^2 + (m^2 + r_0^4)$$

is infinite too (with the convention at the head of Section 2).

THEOREM 3.8. *Let $p_0^2 + bq_0^2 = \frac{(s^2+1)(s^2+2s-1)}{4s^2} r_0^2$. Suppose the set of rational points on the curve $\mathcal{C}_3$ at (9) is infinite. Then the set of rational points on the surface*

$$V_3 :\ (p^2 + bq^2)^2 = X^4 + \frac{r_0^2(s^2 - 1)(s^4 + 2s^3 + 2s^2 - 2s + 1)}{4s^3} X^2 + r_0^4 \frac{(s^2 - 1)^4}{16s^4}$$

is infinite too (with the convention at the head of Section 2).

4. A remark on inhomogeneous representation. The ideas of Sections 2 and 3 can be used to investigate representing the Y-coordinate of points on the curve $\mathcal{C} : Y^2 = A_4X^4 + \cdots + A_0 := f(X)$ by the inhomogeneous quadratic form $ax^2 + by^2 + c$, $a, b, c \in \mathbb{Z}$, $ab \neq 0$. Consider the quartic surface

$$\mathcal{V} : \ (ap^2 + bq^2 + c)^2 = f(X),$$

where we assume $\mathrm{Disc}_X(f) \neq 0$. As before, on multiplying through by a^2, we may suppose without loss of generality that $a = 1$; and again when we refer to $\mathcal{V}(\mathbb{Q})$ being infinite, we mean that $\pi_X(\mathcal{V}(\mathbb{Q}))$ is infinite, where $\pi_X : \mathcal{V}(\mathbb{Q}) \to \mathbb{Q}$ is the projection onto the X-coordinate.

Suppose that (p_0, q_0, X_0) lies on $\mathcal{V}$ with $f(X_0) \neq 0$. Without loss of generality we may assume that $X_0 = 0$ and $p_0q_0 \neq 0$. In particular $A_0 = (p_0^2 + bq_0^2 + c)^2 \neq 0$. To shorten notation, set $m = p_0^2 + bq_0^2 + c$ so that $\mathcal{V}$ takes the form

$$\mathcal{V} : \ (p^2 + bq^2 + c)^2 = A_4X^4 + A_3X^3 + A_2X^2 + A_1X + m^2.$$

To find further points on $\mathcal{V}$, set

$$X = T, \quad p = p_0 + \frac{U + p_0A_1}{4(m - c)m}T, \quad q = q_0 - \frac{p_0U - bq_0^2A_1}{4bq_0(m - c)m}T, \tag{11}$$

where U, T are to be determined. This substitution gives

$$(p^2 + bq^2 + c)^2 - f(X) = \frac{T^2}{256b^2q_0^4(m - c)^2m^4}F(T),$$

where $F(T) = B_0 + B_1T + B_2T^2$ and $B_i \in \mathbb{Z}[U]$ with $\deg_U B_0 = \deg_U B_1 = 2$ and $\deg_U B_2 = 4$. Thus the point (p, q, X) with coordinates given by (11) lies on $\mathcal{V}$ if and only if the equation $F(T) = 0$ has rational roots, which is equivalent to the discriminant $\mathrm{Disc}_T(F)$ being a square. This corresponds to considering the curve in the (U, V) plane given by the equation

$$\mathcal{C} : \ V^2 = B_1^2(U) - 4B_0(U)B_2(U) = -128bq_0^2(m - c)m^3G(U).$$

Here G is monic of degree 6 (and does not contain any odd power of U). In consequence, if G has no multiple roots then $\mathcal{G}$ has only finitely many rational points. We thus seek $\mathrm{Disc}_U(G) = 0$. We have

$$\mathrm{Disc}_U(G) = -2^{42}b^{15}q_0^{30}(m - c)^{12}m^{12}(\mathrm{Disc}_X(f))^2H,$$

where

$$\begin{aligned} H = \ & -8(m - c)m\big(A_1^4 - 256A_4(m - c)^2m^4\big)A_2 + A_1^6 - 64(m - c)^2m^2A_1^3A_3 \\ & + 256(2c - 3m)(m - c)^2m^3A_4A_1^2 - 512(m - c)^3m^5A_3^2, \end{aligned}$$

and $\mathrm{Disc}_U(G) = 0$ if and only if $H = 0$.

We consider two cases:

Case I: $A_1^4-256A_4(m-c)^2m^4=0$. Then

$$A_4=\frac{A_1^4}{256(m-c)^2m^4}\quad\text{and}\quad mH=-2(m-c)\big(A_1^3-16m^3(m-c)A_3\big)^2,$$

whence $A_3=\frac{A_1^3}{16(m-c)m^3}$. Since we are interested only in polynomials f with $\deg_X f\in\{3,4\}$, necessarily $A_1\neq 0$. Summing up: after some simplification, if

$$f_1(X)=\frac{A_1^4}{256(m-c)^2m^4}X^4+\frac{A_1^3}{16(m-c)m^3}X^3+A_2X^2+A_1X+m^2$$

then there exists a non-constant rational map $\varphi_1:\mathcal{C}_1\to\mathcal{V}_1$, where (on replacing U by q_0U)

$$\begin{aligned}(12)\quad \mathcal{C}_1:\ V^2=-2b(m-c)m\big(&mU^4+bm(3A_1^2-8mA_2(m-c))U^2\\ &-2b^2A_1^2((2c-3m)A_1^2+8(m-c)m^2A_2)\big)\end{aligned}$$

and $\mathcal{V}_1:(p^2+bq^2+c)^2=f_1(X)$.

Case II: $A_1^4-256A_4(m-c)^2m^4\neq 0$. We solve the equation $H=0$ with respect to A_2 and get

$$(13)\qquad A_2=\frac{\begin{aligned}&A_1^6+64(m-c)^2m^2A_1^3A_3\\ &+256(2c-3m)(m-c)^2m^3A_1^2A_4-512(m-c)^3m^5A_3^2\end{aligned}}{8m(m-c)(A_1^4-256A_4(m-c)^2m^4)}.$$

Summing up: after some simplification, if

$$f_2(X)=A_4X^4+A_3X^3+A_2X^2+A_1X+m^2,$$

where A_2 is given by (13), then there exists a non-constant rational map $\varphi_2:\mathcal{C}_2\to\mathcal{V}_2$, where (on replacing U by q_0U),

$$(14)\quad \mathcal{C}_2:\ V^2=2bm(m-c)\big(256A_4(m-c)^2m^4-A_1^4\big)(C_4U^4+C_2U^2+C_0)$$

with

$$\begin{aligned}C_4&=A_1^4-256(m-c)^2m^4A_4,\\ C_2&=2b\big(A_1^6-32(m-c)^2m^2(A_3A_1^3+8cmA_4A_1^2-8(m-c)m^3A_3^2)\big),\\ C_0&=b^2\big(A_1^8-64(m-c)^2m^2A_1^5A_3+512(m-c)^2m^3(m-2c)A_1^4A_4\\ &\qquad+1024(m-c)^3m^5A_1^2A_3^2-16384(m-c)^4m^6A_4(A_1A_3-4A_4m^2)\big)\end{aligned}$$

and $\mathcal{V}_2:(p^2+bq^2+c)^2=f_2(X)$.

We can summarize our result in the following:

Theorem 4.1. *Let $m=p_0^2+bq_0^2+c$. Suppose the set of rational points on the curve $\mathcal{C}_1$ at (12) is infinite. Then the set of rational points on the* *surface*

$$\mathcal{V}_1:\ (p^2+bq^2+c)^2=\frac{A_1^4}{256(m-c)^2m^4}X^4+\frac{A_1^3}{16(m-c)m^3}X^3+A_2X^2+A_1X+m^2$$

is infinite too (with the convention at the head of this section).

THEOREM 4.2. *Let $m=p_0^2+bq_0^2+c$. Suppose the set of rational points on the curve $\mathcal{C}_2$ at* (14) *is infinite. Then the set of rational points on the surface*

$$\mathcal{V}_2:\ (p^2+bq^2+c)^2=A_4X^4+A_3X^3+A_2X^2+A_1X+m^2,$$

where A_2 is given by (13), *is infinite too (with the convention at the head of this section).*

EXAMPLE 4.3. Take $(b,c,p_0,q_0)=(1,1,1,1)$ and $(A_1,A_2)=(2,2)$. Then $\varphi_1:\mathcal{C}_1\to\mathcal{V}_1$ where

$$\mathcal{C}_1:\ V^2=130+63U^2-3U^4,$$
$$\mathcal{V}_1:\ (p^2+q^2+1)^2=9+24X+288X^2+16X^3+4X^4$$

is given by

$$(p,q,X)=\left(\frac{-2U^2+U^3-(1+U)V}{U(2+U^2)},\frac{2U^2+U^3-(1-U)V}{U(2+U^2)},\frac{-(2U+V)}{U(2+U^2)}\right).$$

Now $\mathcal{C}_1$ has rational rank 2, with independent points

$$\left(\frac{9}{2},\frac{53}{4}\right),\qquad\left(\frac{152129}{152882},\frac{321697804123}{152882^2}\right),$$

and it follows that the curve $Y^2=9+24X+288X^2+16X^3+4X^4$ has infinitely many points with Y-coordinate represented by the form p^2+q^2+1. We note that the curve $\mathcal{C}_1$ is 2-isogenous to the curve related to $\mathcal{V}_1$.

REMARK 4.4. Essentially the same method as presented in the last three sections can be applied to curves defined by more general equations of the form

$$\mathcal{C}:\ Y^2+f_2(X)Y=f_4(X),$$

where $f_i\in\mathbb{Z}[X]$ and $\deg f_i=i$ for $i=2,4$. However, in order to avoid long computations we have presented our approach only for those $\mathcal{C}$ with $f_2(X)\equiv 0$.

5. The Diophantine equation $Y^2=f(ap^2+bq^2)$ with f cubic. Motivated by the results above, we investigate whether any variation of the method can be used in other situations. Specifically, we consider the question of when the X-coordinates of points on an elliptic curve of type $Y^2=f(X)$,

f cubic, can be represented by the quadratic form $ax_1^2 + bx_2^2$. First, observe that the curve

$$E_1 : \; y^2 = x^3 + Ax^2 + Bx$$

with $A, B \in \mathbb{Q}$, $A^2 - 4B \neq 0$, is 2-isogenous to the curve

$$Y^2 = X^3 - 2AX^2 + (A^2 - 4B)X$$

under $(X, Y) = (y^2/x^2, y(B - x^2)/x^2)$. Accordingly, E_1 is 2-isogenous to the curve

$$E_2 : \; Y^2 = \left(\frac{X-b}{a}\right)^3 - 2A\left(\frac{X-b}{a}\right)^2 + (A^2 - 4B)\left(\frac{X-b}{a}\right)$$

with isogeny given by

$$\varphi : \; E_1 \ni (x, y) \mapsto \left(a\left(\frac{y}{x}\right)^2 + b, \; \frac{y(B - x^2)}{x^2}\right) \in E_2.$$

Thus if E_1 has positive rank, then E_2 has infinitely many rational points (X, Y) with X represented by the form $ap^2 + bq^2$.

Consider the surface

$$\mathcal{W} : \; Y^2 = f(ap^2 + bq^2),$$

where $f(X) = c_3X^3 + c_2X^2 + c_1X + c_0 \in \mathbb{Z}[X]$ is non-singular. Without loss of generality, on multiplying by c_3^2, we may take $c_3 = 1$. As in the case of the surface $\mathcal{V}$ considered in Section 2, when we say that the set $\mathcal{W}(\mathbb{Q})$ is infinite, we mean that the set $\pi_Y(\mathcal{W}(\mathbb{Q}))$ is infinite, where the map $\pi_Y : \mathcal{W}(\mathbb{Q}) \ni (p, q, Y) \mapsto Y \in \mathbb{Q}$ is simply the projection onto the Y-line.

We assume that (p_0, q_0, Y_0) is a rational point on $\mathcal{W}$ with $Y_0 \neq 0$. Now

$$f(0) = c_0 = Y_0^2 - (m^3 + c_2m^2 + c_1m), \qquad m = ap_0^2 + bq_0^2.$$

Computing the discriminant of f with this value of c_0 yields

$$\begin{aligned}(15) \qquad \mathrm{Disc}_X(f) = \; & -27Y_0^4 - 2(c_2 + 3m)(2c_2^2 - 9c_1 - 6c_2m - 9m^2)Y_0^2 \\ & - (c_1 + 2c_2m + 3m^2)^2(-c_2^2 + 4c_1 + 2c_2m + 3m^2).\end{aligned}$$

We will present a method which sometimes allows us to prove that the set $\mathcal{W}(\mathbb{Q})$ is infinite. In order to find more points on $\mathcal{W}$, set

$$(16) \qquad p = T + p_0, \qquad q = UT + q_0, \qquad Y = VT^3 + rT^2 + sT + Y_0,$$

and demand that (p, q, Y) lie on the surface $\mathcal{W}$. This gives

$$Y^2 - f(ap^2 + bq^2) = \sum_{i=1}^{6} C_iT^i,$$

where C_i for $i = 1, \ldots, 6$ is a polynomial in $\mathbb{Q}[U, V, r, s]$ with coefficients depending on p_0, q_0, Y_0. The system $C_1 = C_2 = C_3 = 0$ is linear in V, r, s

and has exactly one solution, of the form

$$V = \frac{Q(U)}{2Y_0^5}, \quad r = \frac{R(U)}{2Y_0^3}, \quad s = \frac{S(U)}{Y_0}, \tag{17}$$

where Q, R, S are polynomials in U with coefficients depending on p_0, q_0, Y_0. Moreover, $\deg P = 3$, $\deg Q = 2$ and $\deg S = 1$. Substituting from (16) into the polynomial $\sum_{i=1}^{6} C_i T^i$, and using V, r, s from (17), we obtain

$$H_U(T) := \frac{A_4}{4Y_0^6} + \frac{A_5}{2Y_0^8}T + \frac{A_6}{4Y_0^{10}}T^2 = 0. \tag{18}$$

It is clear that a necessary condition for solvability of (18) for some fixed $U \in \mathbb{Q}$ is that the discriminant, say $\Delta_U(H)$, of the polynomial H_U should be a square in $\mathbb{Q}$. We see that $\Delta_U(H)$ is a polynomial in U of degree 10. More precisely,

$$(2Y_0^8)^2 \Delta_U(H) = A_5^2 - A_4A_6 = 4H_1(U)H_2(U),$$

where $\deg H_1 = 4$ and $\deg H_2 = 6$. We consider the curve

$$\mathcal{C}: \ W^2 = H_1(U)H_2(U). \tag{19}$$

For general choice of c_1, c_2, Y_0, p_0 and q_0 the curve $\mathcal{C}$ is a hyperelliptic curve of genus 4. From the Faltings Theorem we know that a necessary condition for $\mathcal{C}$ to have infinitely many rational points is that genus$(\mathcal{C}) \le 1$. This immediately implies that the discriminant of the polynomial $H_1(U)H_2(U)$ with respect to U must be 0. In fact, we need to have an equality of the form $H_1(U)H_2(U) = g(U)h(U)^2$, where the degree of g is at most 4.

Since $\mathrm{Disc}_U(H_1H_2) = \mathrm{Disc}_U(H_1)\,\mathrm{Disc}_U(H_2)\,\mathrm{Res}_U(H_1, H_2)^2$, we compute independently the discriminants of H_1, H_2, and the resultant of these two polynomials. To shorten notation, we introduce new quantities:

$$y_0 = Y_0^2, \qquad Z = 3m^2 + 2c_2m + c_1.$$

A quick computation reveals that

$$\mathrm{Disc}_U(H_1) = 2^{12}(ab)^6 m^4 y_0^{10} h_{11} h_{12}^2 h_{13},$$

where

$$\begin{aligned}
h_{11} &= -4(c_2 + 3m)y_0 + Z^2,\\
h_{12} &= 9y_0^2 - 4(3m + c_2)y_0Z + Z^3,\\
h_{13} &= -4(6m + c_2)y_0^3 + 8m(4m + c_2)y_0^2Z\\
&\quad - 4m^2(3m + c_2)y_0Z^2 + Z^2(y_0 - mZ)^2.
\end{aligned}$$

Computation of the expression for $\mathrm{Disc}_U(H_2)$ took much longer; indeed, about 64 hours of CPU time. We have

$$\mathrm{Disc}_U(H_2) = 2^6(ab)^{15} m^{12} y_0^{21} (\mathrm{Disc}_X(f))^2 h_{21}^8 h_{23},$$

where

$$\begin{aligned} h_{21} &= 8y_0^2 - 4(3m + c_2)y_0Z + Z^3, \\ h_{23} &= -y_0^5 + 2m(2c_2^2 + 28c_2m + 98m^2 - Z)y_0^4 \\ &\quad - m(16c_2^2m + 160c_2m^2 + 336m^3 + c_2Z + 11mZ)y_0^3Z \\ &\quad + 8m^2(2c_2^2m + 12c_2m^2 + 18m^3 + c_2Z + 5mZ)y_0^2Z^2 \\ &\quad - m^2(8c_2m + 24m^2 + Z)y_0Z^4 + m^3Z^6. \end{aligned}$$

Finally, the expression for the resultant of the polynomials H_1, H_2 with respect to U is

$$\mathrm{Res}_U(H_1, H_2) = (ab)^{12}m^{12}y_0^{16}g_1^8g_2^2,$$

where

$$\begin{aligned} g_1 &= 8y_0^2 - 4(3m + c_2)Zy_0 + Z^3, \\ g_2 &= 27y_0^2 + 2(c_2 + 3m)(2c_2^2 + 12c_2m + 18m^2 - 9Z)y_0 \\ &\quad - (c_2^2 + 6c_2m + 9m^2 - 4Z)Z^2 \end{aligned}$$

Observe that $h_{21} = g_1$. In consequence, if $h_{21} = 0$ then H_1 and H_2 have a common factor and H_2 has at least one double root.

We are interested only in c_1, c_2, p_0, q_0, Y_0 such that $(ap_0^2 + bq_0^2)Y_0 \neq 0$ and $\mathrm{Disc}_U(H_1H_2) = 0$. Observe that if $\mathrm{Disc}_U(H_1) = 0$ and $\mathrm{Disc}_U(H_2) \neq 0$ then a necessary condition for the curve $\mathcal{C}$ to have genus 1 is $\mathrm{Res}_U(H_1, H_2) = 0$. Similarly, if $\mathrm{Disc}_U(H_1) \neq 0$ and $\mathrm{Disc}_U(H_2) = 0$ then a necessary condition for $\mathcal{C}$ to have genus 1 is that either H_2 is the square of a cubic polynomial, or $\mathrm{Res}_U(H_1, H_2) = 0$. Finally, if $\mathrm{Disc}_U(H_1)\,\mathrm{Disc}(H_2) \neq 0$ then the only possibility for $\mathcal{C}$ to have genus 1 is $\mathrm{Res}_U(H_1, H_2) = 0$.

We perform a case by case analysis of the equations $h_{1j} = 0$ with $j = 1, 2, 3$, $h_{2j} = 0$ with $j = 1, 3$, and $g_2 = 0$.

Case I: $h_{11} = 0$. Then since $y_0 \neq 0$,

$$c_2 = \frac{Z^2 - 12my_0}{4y_0}, \qquad c_1 = Z - 2c_2m - 3m^2 = \frac{6m^2y_0 + 2y_0Z - mZ^2}{2y_0}.$$

The corresponding discriminant $\mathrm{Disc}_X(f)$ is $\frac{1}{2}(Z^3 - 54y_0^2)$, which must be non-zero. Substituting the expressions for c_1, c_2 into $H_1(U)$, we find that $H_1(U)$ has the factor $(ap_0 + bq_0U)^2$, and the cofactor, say G_1 (of degree 2), is irreducible. Now

$$\begin{aligned} \mathrm{Res}_U(H_1, H_2) &= 2^{22}(ab)^{12}m^{12}y_0^{32}(Z^3 - 54y_0^2)^2 \neq 0, \\ \mathrm{Disc}_U(H_2) &= 2^{28}(ab)^{15}m^{12}y_0^{41}(64m^3 - y_0 - 2mZ)(Z^3 - 54y_0^2)^2, \end{aligned}$$

so that necessarily $\mathrm{Disc}_U(H_2) = 0$, implying $y_0 = 2m(32m^2 - Z)$ and $\mathrm{Disc}_X(f) = -\frac{1}{2}(24m^2 - Z)(96m^2 - Z)^2$. Accordingly, $Z \neq 24m^2, 32m^2, 96m^2$. There is now the factor $(q_0 - p_0U)^2$ of $H_2(U)$ and irreducible cofactor $G_2(U)$

of degree 4. Since $\mathrm{Res}_U(H_1,H_2)\neq 0$, it follows that G_1,G_2 cannot have a common root. So $\mathcal{C}$ can have genus 1 only if either G_1 or G_2 has a multiple root. But

$$\begin{aligned}\mathrm{Disc}_U(G_1) &= -2^{14}\cdot 3\cdot (ab)m^6(24m^2-Z)(32m^2-Z)^5,\\ \mathrm{Disc}_U(G_2) &= 2^{48}(ab)^{12}m^{28}(24m^2-Z)^2(32m^2-Z)^{25}(96m^2-Z),\end{aligned}$$

and by the above, neither can be zero. In summary, the vanishing of h_{11} does not lead to any curve of genus 1.

Case II: $h_{12}=0$. Let $\mathcal{C}_{12}$ be the curve

$$\mathcal{C}_{12}:\ h_{12}(c_1,c_2)=0$$

defined over the function field $\mathbb{Q}(m,y_0)$ in the plane (c_1,c_2). The genus of the curve $\mathcal{C}_{12}$ is 0, and because it contains the $\mathbb{Q}(m,y_0)$-rational point at infinity $(-2m:1:0)$, we can find a rational parametrization, for example

$$c_1=-\frac{9my_0^2-2u(3m^2+u)y_0+mu^3}{2uy_0},\qquad c_2=\frac{9y_0^2-12muy_0+u^3}{4uy_0}.$$

With these values of c_1 and c_2, $H_1(U)$ is divisible by the square of a quadratic irreducible over $\mathbb{Q}[u,m,y_0]$. Thus for $\mathcal{C}$ to have genus 1, we require $\mathrm{Disc}_U(H_2)\,\mathrm{Res}_U(H_1,H_2)=0$. This implies the vanishing of at least one of h_{21} $(=g_1)$, h_{23}, or g_2. But with c_1,c_2 as above, we have $h_{21}=-y_0^2\neq 0$; and $g_2=-\mathrm{Disc}_X(f)\neq 0$. We are thus left with $h_{23}=0$, which has become

$$h_{23}=\frac{y_0^4(81my_0^2-4u(9m^2+u)y_0+mu^2(4m^2+u))}{4u^2}.$$

As a polynomial in y_0, there is a non-zero rational root for y_0 precisely when the discriminant of the quadratic factor, namely $4u^3(4u-9m^2)$, is a perfect square. Thus $u(4u-9m^2)=w^2$ for some w. This equation defines a conic over $\mathbb{Q}(m)$ in the (u,w) plane, with parametrization

$$u=\frac{9m^2}{4-v^2},\qquad w=\frac{9m^2v}{4-v^2},$$

where v is a rational parameter. The roots for y_0 are now

$$y_0=\frac{m^3(5-2v)}{(2-v)^2(2+v)},$$

and that obtained by replacing v by $-v$. The corresponding $H_1(U),H_2(U)$ take the form

$$H_1(U)=(4-v^2)(\text{square})l_2(U)^2,\qquad H_2(U)=-ab(2+v)(\text{square})l_1(U)^2l_4(U),$$

for polynomials $l_i(U)$ of degree i which are irreducible over $\mathbb{Q}(v)[m]$. On setting $v = 2 + t$, we have

$$(c_2, c_1, c_0) = \left(-\frac{m(1+t)(-1+13t+5t^2)}{(4+t)t(-1+2t)}, \frac{m^2(1+t)^2(7+4t)}{(4+t)t(-1+2t)}, -\frac{m^3(1+t)^4}{(4+t)t^2(-1+2t)}\right).$$

Summing up, if $f(X) = X^3 + c_2X^2 + c_1X + c_0$, then on setting $(A, B) = (ap_0^2, bq_0^2)$ (with $m = A + B$), and replacing U by $\frac{q_0}{p_0}U$, there exists a non-constant rational map $\psi_1 : \mathcal{C}_1 \to \mathcal{W}_1$, where

$$(20) \qquad \begin{aligned} \mathcal{C}_1 &: W^2 = ABt(k_4U^4 + k_3U^3 + k_2U^2 + k_1U + k_0), \\ \mathcal{W}_1 &: Y^2 = f(ap^2 + bq^2), \end{aligned}$$

and

$$\begin{aligned} k_0 &= -A^2\big((A+B)^2 + 2(A^2 - B^2)t + A(A-3B)t^2 - ABt^3\big), \\ k_1 &= -2A^2Bt(4+t)\big(A + B + (A-B)t\big), \\ k_2 &= AB\big(-2(A+B)^2 + 3(A^2 - 6AB + B^2)t^2 + (A^2 - 4AB + B^2)t^3\big), \\ k_3 &= 2AB^2t(4+t)\big(-(A+B) + (A-B)t\big), \\ k_4 &= -B^2\big((A+B)^2 - 2(A^2 - B^2)t - B(3A-B)t^2 - ABt^3\big). \end{aligned}$$

The discriminant of $\mathcal{C}_1$ is $16(ABmt)^{12}(1+t)^6(4+t)^2(1-2t)$, non-zero since $t \neq 0, -1, -4, 1/2$; and thus $\mathcal{C}_1$ is of genus 1.

Case III: $h_{13} = 0$. Again, this defines a genus zero curve over the field $\mathbb{Q}(m, y_0)$ in the plane (c_1, c_2). There is a triple singular point at infinity $P_0 = (-2m : 1 : 0)$ which determines the following parametrization:

$$(21) \qquad \begin{aligned} c_1 &= \frac{2(9m^2 + u)y_0^3 - 5mu(4m^2 + u)y_0^2 + 2m^2u^2(3m^2 + 2u)y_0 - m^3u^4}{2(mu - y_0)^2y_0}, \\ c_2 &= \frac{1}{2m}(u - 3m^2 - c_1), \end{aligned}$$

where u is a rational parameter. With c_1, c_2 given by (21), we have $\mathrm{Disc}_X(f) = -g_2$, and thus g_2 cannot be zero. Further, H_1 has the factor $(q_0 - p_0U)^2$ and the cofactor, say G_1, is of degree 2 and irreducible over $\mathbb{Q}[m, y_0]$. We can assume that $\mathrm{Disc}_U(G_1) \neq 0$, because $\mathrm{Disc}_U(G_1) = 0$ implies $h_{11}h_{12} = 0$, cases we have already considered. Finally, note that the numerator of h_{23} is a divisor of the polynomial $y_0^6\,\mathrm{Disc}_X(f)$, which implies that $h_{23} = 0$ cannot be zero. To reduce the genus of $\mathcal{C}$ we must therefore have $\mathrm{Disc}_U(H_2) = 0$, i.e. $h_{21} = 0$. We have

$$h_{21} = \frac{4(2y_0 - mu)y_0^3}{(y_0 - mu)^2},$$

and thus $u = 2y_0/m$. In consequence, the polynomial $(a + bU^2)^2$ divides $H_2(U)$, and the square-free part of the polynomial H_1H_2 is of degree 4.

Finally, the coefficients (c_2, c_1, c_0) have become $(-2m + y_0/m^2, m^2, 0)$. Summing up: if

$$f(X) = X\left(X^2 + \left(-2m + \frac{y_0}{m^2}\right)X + m^2\right),$$

then there is a non-constant rational map $\psi_2 : \mathcal{C}_2 \to \mathcal{W}_2$, where

$$(22)\qquad \begin{aligned} \mathcal{C}_2 :\ W^2 = -aby_0(a+bU^2)(a(4am^2p_0^2 - y_0) \\ + 8abm^2p_0q_0U + b(4bm^2q_0^2 - y_0)U^2) \end{aligned}$$

and

$$\mathcal{W}_2 :\ Y^2 = f(ap^2 + bq^2).$$

The second quadratic factor has discriminant $4aby_0(4m^3 - y_0)$, and if $y_0 = 4m^3$, then $f(X)$ becomes $X(X+m)^2$, disallowed. Thus $\mathcal{C}_2$ is of genus 1.

We can henceforth assume that $\mathrm{Disc}(H_1) \neq 0$.

Case IV: $h_{21} = 0$. This equation defines a genus zero curve over the field $\mathbb{Q}(m, y_0)$ in the (c_1, c_2) plane with triple singular point at infinity $P_0 = (-2m : 1 : 0)$. It has the parametrization

$$(23)\qquad c_1 = -\frac{mu^3 - 2u(3m^2+u)y_0 + 8my_0^2}{2uy_0}, \qquad c_2 = \frac{u^3 - 12muy_0 + 8y_0^2}{4uy_0},$$

where u is a rational parameter. With these values of c_1, c_2, we have $H_1(U) = (a+bU^2)G_1(U)$ and $H_2(U) = (a+bU^2)^2G_2(U)$. By our assumptions, necessarily the discriminant of G_2 must vanish, equivalent to the vanishing of h_{23}. We have

$$h_{23} = \frac{y_0^5(16my_0 - u^2)}{u^2},$$

and thus $h_{23} = 0$ if and only if $16my_0 - u^2 = 0$. Set $my_0 = v^2, u = 4v$; then $G_2 = -ab(q_0 - p_0U)^2y_0^5/m$, and the square-free part of $H_1(U)H_2(U)$ is of degree 4. The coefficients (c_2, c_1, c_0) are now

$$\left(\frac{2m^2+v}{2m},\ 3v - 5m^2,\ \frac{(3m^2-2v)(2m^2-v)}{2m}\right).$$

Summing up: if

$$\begin{aligned} f(X) &= X^3 + \left(\frac{2m^2+v}{2m}\right)X^2 - (5m^2-3v)X + \frac{(3m^2-2v)(2m^2-v)}{2m} \\ &= \left(X - \frac{2m^2-v}{2m}\right)(X^2 + 2mX - 3m^2 + 2v) \end{aligned}$$

then there is a non-constant rational map $\psi_3 : \mathcal{C}_3 \to \mathcal{W}_3$, where

$$(24)\qquad \begin{aligned} &\mathcal{C}_3 :\ W^2 = 2ab(a+bU^2)\big(a(2amp_0^2 - v) + 4abmp_0q_0U \\ &\qquad\qquad + b(2mbq_0^2 - v)U^2\big), \\ &\mathcal{W}_3 :\ Y^2 = f(ap^2+bq^2). \end{aligned}$$

The second quadratic factor in $\mathcal{C}_3$ has discriminant $4abv(2m^2 - v)$, and $2m^2 = v$ implies $f(X)$ has a repeated factor. Thus $\mathcal{C}_3$ is of genus 1.

CASE V: $h_{23} = 0$. Due to the assumption $\mathrm{Disc}_U(H_1) \neq 0$, there are two possibilities:

(1) $\mathrm{Res}_U(H_1, H_2) = 0$ and thus $g_2 = h_{23} = 0$ (the possibility $g_1 = 0$ has been covered since $g_1 = h_{21}$).
(2) $\mathrm{Res}_U(H_1, H_2) \neq 0$, in which case the necessary condition for $\mathcal{C}$ to have genus 1 is that H_2 is a square up to multiplication by an element of $\mathbb{Q}(m, Y)$.

In the first instance, the resultant of g_2 and h_{23} with respect to y_0 is

$$(4c_1 - c_2^2)(c_1 + 2c_2m + 3m^2)^{10}(16c_1^2 - 8c_1c_2^2 + c_2^4 - 16c_1c_2m + 6c_2^3m + 3c_1m^2)^2,$$

which must be zero. If $4c_1 = c_2^2$, then either $y_0 = m(c_2 + 2m)^2/4$, or $y_0 = (2c_2 + 3m)(c_2 + 6m)^2/108$, and in both cases $f(X)$ is singular.

If $c_1 + 2c_2m + 3m^2 = 0$, then $y_0 = -4(c_2 + 3m)^3/27$, and $f(X)$ is singular.

If $16c_1^2 - 8c_1c_2^2 + c_2^4 - 16c_1c_2m + 6c_2^3m + 3c_1m^2 = 0$, then this curve of genus 0 has parametrization

$$(c_1, c_2) = \left(\frac{(m+u)^3(-7m+u)}{256m^2}, \frac{(m-u)(m+u)}{8m}\right).$$

Then either $y_0 = (3m - u)^2(5m + u)^3/1024m^2$, or $y_0 = (2m - u)(11m - u)^2 \times (5m + u)^3/(27648m^3)$, and in both cases $f(X)$ is singular.

In the second instance, we form the ideal generated by the coefficients of $d_6x^6 + \cdots + d_0 - d_6(x^3 + px^2 + qx + r)^2$ and obtain the elimination ideal in $d_6, \ldots, d_0$ which Magma tells us has a basis comprising 45 terms. Substitute into the defining polynomials of this basis the coefficients of H_2; this gives 45 polynomials in the variables A $(= ap_0^2)$, B $(= bq_0^2)$, (so $m = A + B$), c_2, y_0, Z, where we seek common zeros. When $Z = 0$, the only solutions that arise correspond to $\mathrm{Disc}(f) = 0$, so henceforth we suppose $Z \neq 0$.

The value $c_2 = \frac{8y_0^2 - 12my_0Z + Z^3}{4y_0Z}$ leads only to $Z^2 = 16my_0$, implying that $y_0 = \frac{Z^2}{16m}$ and

$$(c_2, c_1, c_0) = \left(\frac{8m^2 + Z}{8m}, \frac{-20m^2 + 3Z}{4}, \frac{(6m^2 - Z)(8m^2 - Z)}{16m}\right),$$

with

$$\begin{aligned} f(X) &= X^3 + \frac{8m^2 + Z}{8m}X^2 + \frac{-20m^2 + 3Z}{4}X + \frac{(6m^2 - Z)(8m^2 - Z)}{16m} \\ &= \left(X - \frac{8m^2 - Z}{8m}\right)\left(X^2 + 2mX - \frac{6m^2 - Z}{2}\right). \end{aligned}$$

There is now a non-constant rational map $\psi_4 : \mathcal{C}_4 \to \mathcal{W}_4$ where

$$(25)\qquad \begin{aligned} &\mathcal{C}_4 :\ W^2 = 2ab(a+bU^2)(8m(ap_0+bq_0U)^2 - (a+bU^2)Z),\\ &\mathcal{W}_4 :\ Y^2 = f(ap^2+bq^2). \end{aligned}$$

The second quadratic factor in $\mathcal{C}_4$ has discriminant $4ab(8m^2 - Z)Z$, whose vanishing implies $\mathrm{Disc}(f)$ is zero. Thus $\mathcal{C}_4$ has genus 1.

It remains only to treat the case where $c_2 \neq \frac{8y_0^2-12my_0Z+Z^3}{4y_0Z}$. The problem reduces to finding common zeros of the 45 polynomials, which are of high degree in A, B, g, y_0, Z. This is a tedious computation, requiring careful bookkeeping of the factors of various resultants (to compute some of these resultants took more than 66 hours of CPU time). After much effort and polynomial manipulation, we discover that all the zeros correspond to the vanishing of $\mathrm{Disc}(f)$, so that no further solutions arise.

Case VI: $g_2 = 0$. The equation defines a genus zero curve over the field $\mathbb{Q}(m, Y)$ in the (c_1, c_2) plane, with singular point at infinity $P_0 = (-2m : 1 : 0)$. There is the following parametrization:

$$(26)\qquad c_1 = \frac{(u-m)(u^3-3mu^2+2y_0)}{u^2}, \qquad c_2 = \frac{2u^3-3mu^2+y_0}{u^2},$$

where u is a rational parameter. The corresponding $f(X)$ is singular.

As in the case of Theorems 3.6–3.8 we omit the computational details of checking that the image of the map ψ_i constructed above for $i \in \{1, 2, 3, 4\}$ is not finite provided that the set $\mathcal{C}_i(\mathbb{Q})$ is not finite, and summarize the above case by case analysis in the following:

Theorem 5.1. *Let $i \in \{1, 2, 3, 4\}$ and suppose that the set of rational points on the curve $\mathcal{C}_i$ at* (20), (22), (24), (25) *is infinite. Then the set of rational points on the corresponding surface $\mathcal{W}_i$ is infinite too.*

Example 5.2. Take $(m, v) = (4, -16)$ in Case IV above. This leads to the elliptic curve

$$E_1 :\ Y^2 = X^3 + 2X^2 - 128X + 480 =: f_1(X).$$

Then $E_1(\mathbb{Q}) \simeq \mathbb{Z} \times \mathrm{Tor}(E_1(\mathbb{Q}))$, where the infinite part of $E_1(\mathbb{Q})$ is generated by the point $G_1 = (10, -20)$ and $\mathrm{Tor}(E_1(\mathbb{Q})) \simeq \mathbb{Z}/4\mathbb{Z}$ is generated by the point $P_1 = (4, 8)$. We are interested in rational points on the surface

$$\mathcal{W}_{1,b} :\ Y^2 = f_1(p^2 + bq^2).$$

Take the point P_1 lying on E_1 and follow the method presented. In this case $a = 1$ and $(p_0, q_0, Y_0) = (2, 0, 8)$. Following the construction above gives the genus 1 curve

$$\mathcal{C}_{1,b} :\ W^2 = 2b(bU^2 + 1)(bU^2 + 3)$$

and the map

$$\varphi_{1,b} : \mathcal{C}_{1,b} \ni (U, W) \mapsto (p, q, Y) \in \mathcal{W}_{1,b},$$

given by

$$p = \frac{2b^2U^3 + W}{bU(bU^2 + 1)}, \qquad q = \frac{W - 2bU}{b(bU^2 + 1)}, \qquad Y = \frac{-W(4b^2U^2 + W^2)}{b^3U^3(1 + bU^2)^2}.$$

Suppose that the set $\mathcal{C}_{1,b}(\mathbb{Q})$ is infinite. In this case the image of the set $\mathcal{C}_{1,b}$ by the map $\varphi_{1,b}$ cannot be finite (in the sense mentioned above). Indeed, if $p(U,W)^2 + bq(U,W)^2 = p_0^2 + bq_0^2$ for some fixed p_0, q_0 and the point (U, W) lies on $\mathcal{C}_{1,b}$ then U necessarily satisfies the equation

$$b^2(p_0^2 + bq_0^2 - 6)U^4 + b(p_0^2 + bq_0^2 - 8)U^2 - 6 = 0.$$

Because this equation has at most four rational roots and the set $\mathcal{C}_{1,b}(\mathbb{Q})$ is infinite, clearly the set $\varphi_{1,b}(\mathcal{C}_{1,b}(\mathbb{Q}))$ is infinite.

This proves, for example, that the set of rational points on the surface $\mathcal{W}_{1,1}$ is infinite. Indeed, for $b = 1$ the curve $\mathcal{C}_{1,1}$ is birationally equivalent to the elliptic curve

$$\mathcal{E}_{1,1} : y^2 = x^3 - x^2 - 4x - 2$$

(which is 2-isogenous to E_1). The rank of $\mathcal{E}_{1,1}$ is 1, with $\mathrm{Tor}(\mathcal{E}_{1,1}) \simeq \mathbb{Z}/2\mathbb{Z}$ generated by the point $(-1, 0)$. The infinite part of $\mathcal{E}_{1,1}(\mathbb{Q})$ is generated by the point $P_{1,1} = (-3/4, -1/8)$. This implies that the set of rational points on $\mathcal{C}_{1,1}(\mathbb{Q})$ is infinite and $\varphi_{1,1}(\mathcal{C}_{1,1}(\mathbb{Q}))$ is an infinite subset of $\mathcal{W}_{1,1}(\mathbb{Q})$.

Remark 5.3. One can check that the only values of b such that the curve $\mathcal{C}_{1,b}$ has infinitely many rational points are elements of the set $B = \{1, 2, 3, 6\}$ with corresponding points of infinite order $\{(1, 4), (1/4, 15/4), (1, 12), (2, 90)\}$. Indeed, this is a consequence of the fact that the (finite) set of square-free parts of the integer points lying on the curve $v^2 = u(u + 2)(u + 6)$ (obtained from $\mathcal{C}_{1,b}$ by the substitution $(b, W) = (T/(2u^2), v/(2u))$ is equal to B. As a consequence, the set of those rational points lying on E_1 with X-coordinate represented by the quadratic form $p^2 + bq^2$, where $b \in B$, is infinite.

Remark 5.4. Note that we can use the same method for the question of representations of X-coordinates of rational points on elliptic curves given by the equation

$$\mathcal{C} : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

where a_i are given integers such that the curve $\mathcal{C}$ is non-singular. However, in this case we expect even more difficult computations to arise then the ones encountered in Case V of this section, and thus it was decided to consider only the case of curves $\mathcal{C}$ with $a_1 = a_3 = 0$.

6. Questions and problems. In this section we state some problems and questions which are natural in the light of the results presented above.

Let $f(X) = \sum_{i=0}^{4} c_i X^i \in \mathbb{Q}[x]$ be without multiple roots, and define $\mathcal{C}$ to be the elliptic quartic curve

$$\mathcal{C}:\ Y^2 = f(X),$$

which we assume to have infinitely many rational points. Let

$$G = \{Q_1, \ldots, Q_r, T_1, \ldots, T_m\}$$

be a set of generators for the set $\mathcal{C}(\mathbb{Q})$. Here r is the rank of $\mathcal{C}$, Q_i is of infinite order for $i = 1, \ldots, r$, and T_j is of finite order for $j = 1, \ldots, m$. In particular, for each $Q \in \mathcal{C}(\mathbb{Q})$ we have $Q = \sum_{i=1}^{r}[n_i]Q_i + \sum_{j=1}^{m}[\epsilon_j]T_j$ for some $n_i \in \mathbb{Z}$ and $\epsilon_j \in A_j$, where $A_j \subset \mathbb{N}$ is finite and $|A_j| =$ order of the point T_j for $j = 1, \ldots, m$.

Assume further that the set of rational points on the surface

$$\mathcal{V}:\ (ap^2 + bq^2)^2 = f(X)$$

is infinite, and define the set

$$\mathcal{S} := \Big\{(p, q, \mathbf{n}, \boldsymbol{\epsilon}) \in \mathbb{Q} \times \mathbb{Q} \times \mathbb{N}^r \times A_1 \times \ldots \times A_m :\ ap^2 + bq^2 = \pi_Y\Big(\sum_{i=1}^{r}[n_i]Q_i + \sum_{j=1}^{m}[\epsilon_j]T_j\Big)\Big\},$$

where to shorten notation we write $\mathbf{n} = (n_1, \ldots, n_r)$, $\boldsymbol{\epsilon} = (\epsilon_1, \ldots, \epsilon_m)$, and where $\pi_Y : \mathbb{Q}^2 \to \mathbb{Q}$ is projection onto the Y-coordinate. In particular, our assumptions imply that the set $\mathcal{S}$ is infinite. Moreover, we assume that the method presented in Sections 2 and 3 works for f, in that the related curve $\mathcal{C}'$ has infinitely many rational points and there is a map $\varphi : \mathcal{C}' \to \mathcal{C}$ given by $\varphi = (\varphi_1, \varphi_2)$ with φ_2 being of the form $ap^2 + bq^2$ for some rational functions p, q.

We ask the following:

QUESTION 6.1. *What part of the set $\mathcal{S}$ is covered by $\varphi(\mathcal{C}'(\mathbb{Q}))$?*

QUESTION 6.2. *Let $f \in \mathbb{Q}[X]$ be as above and suppose that the curve $\mathcal{C}$ has infinitely many rational points. Let $\mathcal{P}$ be the set of pairs (a, b) of square-free integers such that the quadratic form $ap^2 + bq^2$ is irreducible over $\mathbb{Q}$ and the set of rational points on the surface*

$$\mathcal{V}_{a,b}:\ (ap^2 + bq^2)^2 = f(X)$$

is infinite. Can $\mathcal{P}$ be infinite?

Further, for any given pair $(a, b) \in \mathbb{Z} \setminus \{(\pm 1, \mp 1\}$ of square-free integers, is it possible to find infinitely many quartic polynomials $f \in \mathbb{Z}[X]$ such that the surface $\mathcal{V}_{a,b}$ has infinitely many rational points? (*We assume that the polynomial f is not divisible by the fourth power of a non-zero integer $\neq 1$.*)

Problem 6.3. *Study analogs of Questions* 6.1 *and* 6.2 *related to representation by a quadratic form of the* X*-coordinate of rational points on the elliptic curve* $\mathcal{E} : Y^2 = f(X)$*, where* f *is a cubic polynomial without multiple roots.*

Consider the curve $E : Y^2 = f(X)$ with $f \in \mathbb{Z}[X]$, where f is without multiple roots and $\deg f = 3, 4$ depending on whether we ask about representations of X-coordinates or Y-coordinates of rational points on E by a binary quadratic form. Denote this set of represented coordinates by $S(E)$. It was noted that in each example of the application of our method throughout the paper, (part of) the set $S(E)$ is parametrized by a certain curve $\mathcal{C}$ of genus 1 *isogenous* to E. This suggests the following:

Question 6.4. *Let* $E : Y^2 = f(X)$ *where* $f \in \mathbb{Z}[X]$ *is without multiple roots and* $\deg f = 3$ *or* 4*. Suppose that the set* $S(E)$ *defined above is infinite. Does there exist a genus* 1 *curve* $\mathcal{C}$ *with infinitely many rational points and an isogeny* $\varphi : \mathcal{C} \to E$ *such that* $\pi(\varphi(\mathcal{C}(\mathbb{Q}))) \subset S(E)$*? (Here,* $\pi = \pi_X$ *or* $\pi = \pi_Y$ *depending on whether we are asking about representability of* X*- or* Y*-coordinate.)*

Finally, we ask the following:

Question 6.5. *Does there exist a quartic polynomial* f_4 *(without multiple roots), and a binary cubic form* $h(x, y) \in \mathbb{Z}[x, y]$*, such that the surface*

$$\mathcal{S}_1 : \ h(p, q)^2 = f_4(X)$$

has infinitely many non-trivial rational points? Does there exist a cubic polynomial f_3 *(without multiple roots), and a binary cubic form* $h(x, y) \in \mathbb{Z}[x, y]$*, such that the surface*

$$\mathcal{S}_2 : \ Y^2 = f_3(h(p, q))$$

has infinitely many non-trivial rational points?

Acknowledgements. All computations for this paper were carried out using Magma [1] and Mathematica [4].

The research of the second author was partially supported by the grant of the Polish National Science Centre no. UMO-2012/07/E/ST1/00185.

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.

[2] D. V. Chudnovsky and G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Adv. Appl. Math. 7 (1986), 385–434.

[3] G. Cornelissen and K. Zahidi, *Elliptic divisibility sequences and undecidable problems about rational points*, J. Reine Angew. Math. 613 (2007), 1–33.

[4] Wolfram Research, Inc., *Mathematica, Version 9.0*, Champaign, IL, 2012.

Andrew Bremner
School of Mathematics and Statistical Sciences
Arizona State University
Tempe, AZ 85287-1804, U.S.A.
E-mail: bremner@asu.edu

Maciej Ulas
Institute of Mathematics
Jagiellonian University
Łojasiewicza 6
30-348 Kraków, Poland
E-mail: Maciej.Ulas@im.uj.edu.pl
maciej.ulas@gmail.com