SIEVING FOR RATIONAL POINTS
ON HYPERELLIPTIC CURVES

SAMIR SIKSEK

To Shaheen

ABSTRACT. We give a new and efficient method of sieving for rational points
on hyperelliptic curves. This method is often successful in proving that a
given hyperelliptic curve, suspected to have no rational points, does in fact
have no rational points; we have often found this to be the case even when our
curve has points over all localizations $\mathbb{Q}_p$. We illustrate the practicality of the
method with some examples of hyperelliptic curves of genus 1.

1. INTRODUCTION

By a hyperelliptic curve we mean a curve of the form

$$(1) \qquad C \; : \; y^2 = f(x),$$

where f is a nonconstant polynomial in $\mathbb{Z}[x]$ with no repeated roots. We restrict our
attention to the case where the degree of f is even, though doubtless the methods of
this paper can easily be adapted to the case where f has odd degree, and presumably
with more trouble to other classes of algebraic curves. We are concerned with
finding rational points on (1), and with proving that there are no rational points
if this seems to be the case. Using what is essentially an algorithm due to Birch
and Swinnerton-Dyer, one can check whether equation (1) is everywhere locally
soluble; this is explained in Section 3. Trivially, this is a necessary condition for
the existence of rational points, and so we assume that equation (1) is everywhere
locally soluble. It is trivial to check if the points at infinity on (1) are rational, and
thus we may restrict our attention to points on the affine model. By computing the
real roots of f, we can write down a finite list of disjoint real intervals $I_1, \ldots, I_m$
such that for any real number x we have that $f(x) \geq 0$ if and only if $x \in I_j$ for
some j. We let I be one of these intervals, and we look at rational points (x, y) on
the affine curve C, such that $x \in I$. We can write

$$x = \frac{X}{Z} \; , \; y = \frac{Y}{Z^n},$$

where $2n = d$ is the degree of f and X, Y, Z are integers satisfying

(2)   X, Z are coprime integers, $Z \geq 1$, and $\dfrac{X}{Z} \in I$.

Let F be the homogeneous binary form satisfying $F(X, Z) = Z^d f(X/Z)$. Then

(3) $Y^2 = F(X, Z).$

In this paper we use quadratic reciprocity to derive finite sets of congruences for expressions of the form $\beta X - \alpha Z$ for suitably chosen pairs of integers α, β. It is these congruences, gathered for many such pairs α, β, which will help us sieve for solutions to (3) satisfying (2), which in turn correspond to rational points on (1). In practice, we have often found that these congruences are "incompatible with the curve" (a term explained later), and this leads to a proof of the nonexistence of rational points on the curve. This is illustrated by the example in Section 4. Even when the congruences derived are "compatible with the curve" they can still help in finding rational points as in the example in Section 9.

The basic idea in this paper is motivated by Lind's counterexample to the Hasse principle (see [Sil], pages 316–318, or [Ca2], page 284). I am grateful to Nigel Smart for many helpful discussions during the course of writing this paper, and to John Cremona and the referee for pointing out many corrections and improvements in both the presentation and contents of this paper.

2. QUADRATIC RECIPROCITY

Suppose that α, β is a given pair of coprime integers such that

(4) $F(\alpha, \beta) = \gamma \delta^2,$

where γ, δ are nonzero integers, and γ is square-free and not equal to 1. We want to derive information about the prime divisors of $\beta X - \alpha Z$ where (X, Z, Y) is any point on (3) satisfying the conditions (2). As we will see, this will allow us to write down a finite set of congruences for $\beta X - \alpha Z$.

Lemma 2.1. *Suppose the triple* (X, Z, Y) *satisfies* (2) *and* (3). *Suppose* $p^r | (\beta X - \alpha Z)$, *where p is a prime and $r \geq 1$. Then $\gamma \delta^2$ is congruent to a square modulo p^r.*

Proof. Suppose that $p^r | (\beta X - \alpha Z)$, where p is a prime and $r \geq 1$. Since X, Z are coprime, and α, β are coprime, it follows that there exists an integer λ, not divisible by p, such that

$$X \equiv \lambda \alpha, \ Z \equiv \lambda \beta \pmod{p^r}.$$

Combining these congruences with the equations (3) and (4) we get

(5) $Y^2 = F(X, Z) \equiv \lambda^{2n} F(\alpha, \beta) = \gamma \delta^2 . \lambda^{2n} \pmod{p^r}.$

The lemma now follows.   □

We need the following standard result from the theory of quadratic reciprocity.

Lemma 2.2. *Suppose as above that γ is a square-free integer, $\gamma \neq 0, 1$, and let*

$$N = \begin{cases} |\gamma| & \text{if} \ \ \gamma \equiv 1 & \pmod 4, \\ 4|\gamma| & \text{if} \ \ \gamma \equiv 2 \ \text{or} \ 3 & \pmod 4. \end{cases}$$

Then there exists a unique subgroup H of $(\mathbb{Z}/N\mathbb{Z})^*$ such that if p is any prime not dividing N, then γ is a square modulo p if and only if the reduction of p modulo N

is contained in H. Moreover H has index 2 in $(\mathbb{Z}/N\mathbb{Z})^*$. Further $-1 \in H$ if and only if $\gamma > 0$.

Proof. The Lemma follows trivially from the definition and standard properties of of the Kronecker-Jacobi symbol (see [Cohen], page 28). Using these same properties, the subgroup H can be computed easily. □

Before proceeding further, we set the following notations. If R is a unique factorization domain, we denote by $\mathbb{P}C(R)$ the set of triples (X, Z, Y) in R^3 such that X and Z are coprime and equation (3) is satisfied. Moreover we let

$R(p)$ be the quantity sup $\{v_p(\beta X - \alpha Z) \mid (X, Z, Y) \in \mathbb{P}C(\mathbb{Z}_p)\}$,

$p_1, \ldots, p_l$ be the distinct primes dividing N,

$q_1, \ldots, q_m$ be the distinct primes dividing 2δ which do not divide N and whose reduction modulo N is *not* contained in H.

Finally we define B to be the set of all products $p_1^{r_1} \cdots p_l^{r_l} q$ such that
- $0 \leq r_i \leq R(p_i)$ for $i = 1, \ldots, l$,
- $q = 1$ or $q = q_j$ for some j such that $R(q_j) \geq 1$.

Lemma 2.3. *For any prime p dividing N we have $R(p) \leq 2v_p(\delta) + 1$. It trivially follows that the set B is finite.*

Proof. Suppose first that p is odd. Now p divides N and hence it divides γ exactly once. Suppose that $(X, Z, Y) \in \mathbb{P}C(\mathbb{Z}_p)$ and let $e = v_p(\delta)$, $r = v_p(\beta X - \alpha Z)$. If $r \geq 2e + 2$, then by equation (5) we get that

$$Y^2 \equiv p^{2e+1} \times (p\text{-adic unit}) \pmod{p^{2e+2}}$$

giving a contradiction. This proves Lemma 2.3 when p is odd.

Suppose now that $p = 2$. The proof is exactly the same as above in the case $2|\gamma$. So suppose that γ is odd. Since 2 divides N we must have that $\gamma \equiv 3 \pmod 4$. Thus if $r \geq 2e + 2$, then

$$Y^2 \equiv 3 \times 2^{2e} \pmod{2^{2e+2}},$$

which implies that 3 is a square modulo 4 giving a contradiction. This completes the proof. □

We come now to our main theorem which gives us our possible congruences for $\beta X - \alpha Z$.

Theorem 2.4. *Let I be an interval in $\mathbb{R}$ such that $f(x) \geq 0$ for all $x \in I$. Let*

$$\zeta = \begin{cases} -1 & \text{if } \beta w - \alpha \text{ is strictly negative for all } w \text{ in } I, \\ 1 & \text{otherwise.} \end{cases}$$

Moreover suppose that (X, Z, Y) is an integer triple satisfying (3) and (2). Then

(6) $$\beta X - \alpha Z \equiv \zeta P h \pmod{P.N}$$

for some $P \in B$, and $h \in H$.

Proof. We first note that $\beta X - \alpha Z$ cannot be zero for otherwise it is easy to deduce that γ is a square, contradicting our assumptions. Write

$$(7) \qquad |\beta X - \alpha Z| = p_1^{r_1} \cdots p_l^{r_l} M,$$

where M is a positive integer coprime to N, and $r_1, \ldots, r_l$ are nonnegative. We want to write down a set of possible congruences for $|\beta X - \alpha Z|$. We begin by doing this for M.

We claim that M satisfies one of the following congruences: either

$$M \equiv h \pmod{N}$$

for some $h \in H$, or

$$M \equiv hq_j \pmod{Nq_j}$$

for some $h \in H$ and some q_j satisfying $R(q_j) \geq 1$. To see this, suppose that q is a prime dividing M. Recall that M is coprime to N and thus q does not divide γ. By Lemma 2.1 we see that if q does not divide 2δ, then γ is a quadratic residue modulo q and so by Lemma 2.2 the reduction of q modulo N is in H. Hence we can write

$$M = q_1^{s_1} \cdots q_m^{s_m} M',$$

where the reduction of M' modulo N is contained in H.

Recall that H is a subgroup of index 2 in $(\mathbb{Z}/N\mathbb{Z})^*$. Thus if $\sum s_j \equiv 0 \pmod{2}$, then the reduction of M modulo N is in H; that is $M \equiv h \pmod{N}$ for some $h \in H$.

Otherwise $M = q_j M''$ for some $1 \leq j \leq m$, where $M'' \equiv h \pmod{N}$ for some $h \in H$. Thus $M \equiv h_i q_j \pmod{Nq_j}$, and as q_j divides M and thus divides $\beta X - \alpha Z$, it follows from the definition of R above that $R(q_j) \geq 1$. This establishes our claim.

Next we observe from (7), again by the definition of R, that $0 \leq r_i \leq R(p_i)$ for $i = 1, \ldots, l$. Thus

$$|\beta X - \alpha Z| \equiv P.h \pmod{P.N}$$

for some $P \in B$ and $h \in H$.

The theorem now follows trivially in the case that $w \to \beta w - \alpha$ has a fixed sign over the interval I. Thus we may suppose that β is nonzero and $\frac{\alpha}{\beta}$ is contained in I. But by assumption $f(x) \geq 0$ for all x in I. Thus $\gamma\delta^2 = \beta^{2n} f(\alpha/\beta) \geq 0$, where $2n$ is the degree of f. Hence as γ, δ are nonzero it follows that γ is positive, and so by Lemma 2.2 that $-1 \in H$. Thus multiplication by -1 simply permutes the elements of H, and so

$$\beta X - \alpha Z \equiv P.h \pmod{P.N}$$

for some $P \in B$ and $h \in H$. This completes the proof of Theorem 2.4. $\qquad \square$

3. Local solubility I

Given a hyperelliptic curve C defined by equation (1), where as before f is a square-free nonconstant polynomial in $\mathbb{Z}[x]$ with even degree, we would like to be able to test whether C has points over all localizations of $\mathbb{Q}$ (by which we mean $\mathbb{R}$ and $\mathbb{Q}_p$ for finite primes p). Testing for the existence of real points is trivial; we merely have to check that the polynomial f is not totally negative.

Recall that the genus of C is $g = n - 1$, where $2n = d$ is the degree of f. Suppose now that p does not divide 2Δ, where Δ is the discriminant of f. Then C has good

reduction at p and its genus over the finite field $\mathbb{F}_p$ is still g. Thus by a Theorem of Weil (the so-called Riemann hypothesis for function fields, see [Cal], page 342), we know that we need only test that $C(\mathbb{Q}_p)$ is nonempty for the finitely many primes p which either divide 2Δ or satisfy $p < 4g^2$.

Thus far everything is standard. Now we need a method of testing for a given prime p whether or not C has points over $\mathbb{Q}_p$. Here we use an algorithm due to Birch and Swinnerton-Dyer given in [Cre1]. The algorithm is stated on page 81 of [Cre1] for the case $d = 4$. However, it is pointed out (page 82 of [Cre1]) that the same algorithm works for any degree with essentially trivial changes. In fact the algorithm does much more than just testing for local solubility.

Lemma 3.1. *For any $x_0 \in \mathbb{Z}_p$, and $r \geq 0$, we can determine whether or not there exists $x \in \mathbb{Z}_p$ with $v_p(x - x_0) \geq r$ and $f(x) = y^2$ for some $y \in \mathbb{Z}_p$. If Δ is the discriminant of f and $s = v_p(\Delta)$, then this decision can be made in time $O\left(p^{s+1} \log(p)^2\right)$.*

Proof. The first part of the lemma is an elementary consequence of Hensel's Lemma. The details are given in the algorithm $\mathbb{Z}_p$-`soluble` in [Cre1], page 82, which is originally due to Birch and Swinnerton-Dyer. The book does not give a complexity estimate but it is not hard to supply one. Assume p is odd, the case $p = 2$ being similar. The algorithm involves invoking a certain "subalgorithm" at most p^{s+1} times. In this "subalgorithm" one is required to decide if a certain p-adic integer is a p-adic square; i.e., that its p-adic valuation is even, and that what is left after the powers of p have been removed is a square modulo p. The estimate given in the lemma is now clear once we recall that a Legendre symbol $\left(\frac{a}{p}\right)$ can be computed in $O(\log(p)^2)$ (see [Cohen], page 31). □

3.1. **Computing $R(p)$.** We start by rephrasing Lemma 3.1 as follows:

Lemma 3.2. *Given coprime integers α, β, a prime p and an integer $r \geq 0$, we can determine whether or not there exists $(X, Z, Y) \in \mathbb{P}C(\mathbb{Z}_p)$ such that $p^r | (\beta X - \alpha Z)$. Again, if Δ is the discriminant of f and $s = v_p(\Delta)$, then this decision can be made in time $O\left(p^{s+1} \log(p)^2\right)$.*

Proof. Suppose first that p does not divide α. Let g be the reverse polynomial to f; that is $g(x) = x^d f(1/x)$. It is then easy to show that there exists $(X, Z, Y) \in \mathbb{P}C(\mathbb{Z}_p)$ with $p^r | (\beta X - \alpha Z)$ if and only if there exists x in $\mathbb{Z}_p$ such that $v_p(x - \frac{\beta}{\alpha}) \geq r$ and $g(x)$ is a p-adic square. By Lemma 3.1 this decision can be made and in the time stated.

If p divided α, then p does not divide β and we proceed similarly. □

Corollary 3.3. *Suppose α, β, γ, δ are integers satisfying (4), where α, β are coprime, δ is nonzero, and γ is square-free and not equal to 0 or 1. Let p be a prime. Then $R(p)$ is effectively computable. If s is as in the previous lemma, then this computation can be carried out in time $O\left((v_p(\delta) + 1)\, p^{s+1} \log(p)^2\right)$.*

Proof. It follows from the definition of R and the proof of Lemma 2.1 that $R(p) = \infty$ if and only if γ is a p-adic square.

Suppose now that γ is not a p-adic square. Then we can simply continue testing, for each $r \geq 0$, if there exists $(X, Z, Y) \in \mathbb{P}C(\mathbb{Z}_p)$ such that $p^r | (\beta X - \alpha Z)$. The greatest value of r for which the answer is yes is $R(p)$, and thus $R(p)$ is effectively computable. It remains to prove the complexity estimate given. From equation (5),

since γ is not a p-adic square, $r \leq 2v_p(\delta)$ if p is odd and $r \leq 2v_p(\delta) + 2$ if $p = 2$. The estimate can now be trivially deduced from the previous lemma. $\qquad\square$

4. AN EXAMPLE

Consider the elliptic curve

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

This is the first curve in the tables of [Cre1] whose Mordell-Weil group is torsion-free but whose Tate-Shafarevich group is nontrivial. In [Me,Si,Sm] the authors used the method of further descents to show that all three nontrivial 2-coverings of E have no rational points and thus that the curve has rank 0 and that the 2-primary part of the Tate-Shafarevich group of the curve has order 4. This has also been proved in [Ca3] using a different method. The results are in agreement with the values predicted by the Birch and Swinnerton-Dyer conjectures. We show the same result using our method which we claim is the simplest since, unlike the methods used in [Me,Si,Sm] and [Ca3], it does not involve any number field arithmetic. The 2-coverings are

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

and were in fact generated by Cremona's program `mwrank`; see [Cre1]. Let us consider the first 2-covering above and denote it by C. Write

$$
\begin{aligned}
f(x) &= -4x^4 + 4x^3 + 92x^2 - 104x - 727, \\
F(X, Z) &= -4X^4 + 4X^3Z + 92X^2Z^2 - 104XZ^3 - 727Z^4.
\end{aligned}
$$

By considering the roots of f we see that $f(x)$ is nonnegative if and only if $x \in I$, where $I = [-3.31353, -3.31277]$ (the end-points of the interval have been rounded to five decimal places). Clearly C has no points at infinity and so it is sufficient to show that there are no triples (X, Z, Y) satisfying (2) and (3). We have programmed the algorithms in this paper (including the ones to follow) using the package `pari/gp` and ran them on a SGI workstation.

First we looked at all pairs of coprime α, β such that $-100 \leq \alpha \leq 100$ and $0 \leq \beta \leq 100$. We expressed $F(\alpha, \beta)$ in the form $\gamma\delta^2$ with γ square-free, and noted all the quadruples with $|\gamma| \leq 10$. We found the following values.

α	β	γ	δ
1	0	-1	2
-53	16	-1	2
-27	8	-1	58
-33	8	-1	838
-10	3	-7	1
5	2	-7	34

It took 17 seconds to produce this table, and only about 0.4 seconds for our program based on the algorithm in Section 8 to show that there are no triples (X, Z, Y) satisfying (2) and (3); hence C has no rational points. For illustration we do some of the calculations explicitly. Suppose (X, Z, Y) satisfies (2) and (3). Let us take the second quadruple in the above table, that is $\alpha = -53$, $\beta = 16$, $\gamma = -1$, $\delta = 2$, and determine the possible congruences for $16X + 53Z$ using the method in Section 2;

we follow the notation of that section. Here $N = 4$ and $H = \{1\}$. Note that the only prime dividing $2\gamma\delta = -4$ is 2. Hence all the odd primes dividing $16X + 53Z$ must be congruent to 1 modulo 4. Further our program tells us that $R(2) = 1$; that is, the power of 2 dividing $16X + 53Z$ does not exceed 2. However it is easy to show that 4 does not divide $16X + 53Z$. Otherwise 4 divides Z, and by considering the coefficients of F in $Y^2 = F(X, Z)$ it follows that 16 divides $Y^2 + 4X^2$. This implies that 2 divides X contradicting the fact that X and Z must be coprime (since (X, Z, Y) satisfies (2)).

Thus $|16X + 53Z| \equiv 1 \pmod 4$ or $|16X + 53Z| \equiv 2 \pmod 8$. However since by assumption (X, Z, Y) satisfies (2), we know that $Z \geq 1$ and $X/Z \in I$. It is easy to see that $16x + 53$ is negative for all $x \in I$. Thus $16X + 53Z$ is negative. Hence either $16X + 53Z \equiv 3 \pmod 4$ or $16X + 53Z \equiv 6 \pmod 8$, or equivalently either $Z \equiv 3 \pmod 4$ or $Z \equiv 6 \pmod 8$. Similarly, using the first quadruple in the above table, either $Z \equiv 1 \pmod 4$ or $Z \equiv 2 \pmod 8$. This contradiction shows that our first 2-covering does not have any rational points.

Our program also showed that the second and third 2-coverings do not have any rational points in a few seconds.

5. Solving a general inhomogeneous system of linear equations over $\mathbb{Z}$ and $\mathbb{Z}_p$

We will need to solve systems of simultaneous inhomogeneous linear equations over some principal ideal domain R which will be either $\mathbb{Z}$ or $\mathbb{Z}_p$ (where p is some prime). I am indebted to John Cremona for showing me how to do this using Smith Normal Forms. Suppose our system is given by

$$(8) \qquad\qquad \mathcal{A}\mathbf{x} = \mathbf{b},$$

where $\mathbf{b} \in R^m$ and $\mathcal{A}$ is an $m \times n$ matrix with entries from R. By the standard theory of Smith Normal Forms (see, for example, [Cohn], page 322), one can compute invertible square matrices U, V of orders m and n, respectively, over R, such that $U\mathcal{A}V$ has a diagonal submatrix in the top left-hand corner and zeros elsewhere; the diagonal has entries $d_i \neq 0$ for $i = 1, \dots, r$, and d_i divides d_{i+1} for $i = 1, \dots, r-1$ (here r is the rank of A).

Lemma 5.1. *With the notation as above, let $S = U\mathcal{A}V$ and $\mathbf{b}' = U\mathbf{b}$. Let $b'_1, \dots, b'_m$ be the entries of $\mathbf{b}'$, and let $\mathbf{e}_j$ be the element of R^n which has 1 in the jth position and 0 elsewhere. Then equation (8) has solutions if and only if d_i divides b'_i for $i = 1, \dots, r$. If this is the case, let $\mathbf{y}_0$ be the (column) vector in R^n with entries $b'_1/d_1, \dots, b'_r/d_r, 0, \dots, 0$, and let $\mathbf{x}_0 = V\mathbf{y}_0$. Then the general solution to equation (8) is $\mathbf{x} = \mathbf{x}_0 + \sum_{j=1}^{n-r} k_j\mathbf{x}_j$ for any $k_1, \dots, k_{n-r}$ in R, where $\mathbf{x}_j = V\mathbf{e}_{j+r}$ for $j = 1, \dots, n-r$.*

Proof. Write $\mathbf{y} = V^{-1}\mathbf{x}$. Then $\mathcal{A}\mathbf{x} = \mathbf{b}$ if and only if $S\mathbf{y} = \mathbf{b}'$. The rest is now trivial. $\qquad\square$

6. Inhomogeneous congruences

Later in this paper, we need to parametrize the solutions to systems of simultaneous congruences of the form

$$(9) \qquad\qquad \beta_i X - \alpha_i Z \equiv c_i \pmod{d_i}$$

for $i = 1, \ldots, n$. Here α_i, β_i, c_i, d_i are all integers. Each $d_i \geq 2$ and each pair α_i, β_i are coprime.

Lemma 6.1. *Let A be the set of $\left(\begin{smallmatrix} X \\ Z \end{smallmatrix}\right) \in \mathbb{Z}^2$ which satisfies the system of congruences (9). Suppose A is nonempty. Then there exists vectors $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w} \in \mathbb{Z}^2$ such that*

$$(10) \qquad\qquad A = \{\mathbf{u} + \lambda\mathbf{v} + \mu\mathbf{w} : \lambda,\ \mu \in \mathbb{Z}\},$$

$\mathbf{v}$ *and* $\mathbf{w}$ *being linearly independent. Moreover if we write*

$$(11) \qquad\qquad \mathbf{v} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}, \ \mathbf{w} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$$

and we let $d = \mathrm{lcm}(d_1, \ldots, d_n)$, then d divides $w_2 v_1 - w_1 v_2$.

Proof. The lemma is elementary except perhaps for the last part. Let $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$ be as in the statement of the lemma. Let B_i (for $i = 1, \ldots, n$) be the set of solutions in $\mathbb{Z}^2$ to the single congruence $\beta_i X - \alpha_i Z \equiv 0 \pmod{d_i}$. Let B be the intersection of $B_1, \ldots, B_n$. Clearly B has $\mathbb{Z}$-basis $\mathbf{v}$, $\mathbf{w}$, and is a submodule of each B_i which is in turn a submodule of $\mathbb{Z}^2$, all having rank 2. Thus the index of each B_i in $\mathbb{Z}^2$ divides the index of B in $\mathbb{Z}^2$. Now the latter index is $w_2 v_1 - w_1 v_2$, while for each i, the former index is d_i (for this we need the assumption, made above, that each pair α_i, β_i is coprime). The lemma now follows. $\qquad\square$

To parametrize the solutions to the system (9), we write $X_1 = X$, $X_2 = Z$ and then solve the simultaneous equations

$$(12) \qquad\qquad \beta_i X_1 - \alpha_i X_2 + d_i X_{i+2} = c_i, \ i = 1, \ldots, n$$

using the method explained above in Section 5. It is clear that the $n \times (n + 2)$ matrix with ith row $\beta_i, -\alpha_i, 0, \ldots, 0, d_i, 0, \ldots, 0$, where the d_i is in the $i + 2$ place $(i = 1, \ldots, n)$, has rank n, and therefore its kernel has rank 2. Thus for (12), if it has a solution at all we are able to write down vectors $\mathbf{u}'$, $\mathbf{v}'$, $\mathbf{w}' \in \mathbb{Z}^{n+2}$, with $\mathbf{v}'$, $\mathbf{w}'$ independent, such that $\mathbf{X}$ is a solution to (12) if and only if $\mathbf{X} = \mathbf{u}' + \lambda\mathbf{v}' + \mu\mathbf{w}'$ for some λ, $\mu \in \mathbb{Z}$. We let $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$ be the vectors in $\mathbb{Z}^2$ obtained from the first two entries of $\mathbf{u}'$, $\mathbf{v}'$, $\mathbf{w}'$, respectively. These can be taken to be the $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$ in the above lemma.

7. Local solubility II

It is apparent from above that we should be looking for triples (X, Z, Y) which satisfy (2) and (3) as well as a system of linear congruences such as (9). Clearly a necessary condition for the existence of such solutions is that (9) should itself have solutions. We assume that this is the case and that we have parametrized the solutions as in Lemma 6.1. Another necessary condition is that for each prime p there exists $(X, Z, Y) \in \mathbb{P}C(\mathbb{Z}_p)$, such that

$$\begin{pmatrix} X \\ Z \end{pmatrix} = \mathbf{u} + \lambda\mathbf{v} + \mu\mathbf{w}$$

for some λ, μ in $\mathbb{Z}_p$ (where we abuse notation by letting $\mathbb{Z}_\infty = \mathbb{R}$). We would like to test whether this is the case for all primes p. We write $\mathbf{v}$, $\mathbf{w}$ as in (11). If $p = \infty$ or if p is finite and does not divide $w_2 v_1 - w_1 v_2$, then it is clear that every element of $\mathbb{Z}_p^2$ can be written in the form $\mathbf{u} + \lambda\mathbf{v} + \mu\mathbf{w}$ for some λ, $\mu \in \mathbb{Z}_p$. However, we

have made the assumption that C has points over all localizations of $\mathbb{Q}$, thus it is sufficient to check solubility only for the finitely many primes dividing $w_2 v_1 - w_1 v_2$.

Then we want to ask for each prime p dividing $w_2 v_1 - w_1 v_2$, does there exist λ, $\mu \in \mathbb{Z}_p$ such that if we let

$$
\begin{aligned}
X &= u_1 + \lambda v_1 + \mu w_1, \\
Z &= u_2 + \lambda v_2 + \mu w_2,
\end{aligned}
$$

then $\min(v_p(X), v_p(Z)) = 0$ and $F(X, Z)$ is a p-adic square? We can answer yes precisely when we can positively answer one of the following two questions:

1. Is there a solution to the simultaneous equations

$$
(13) \qquad \left.\begin{aligned}
x &= \epsilon u_1 + \lambda v_1 + \mu w_1 \\
1 &= \epsilon u_2 + \lambda v_2 + \mu w_2
\end{aligned}\right\}
$$

with x, λ, $\mu \in \mathbb{Z}_p$ and $\epsilon \in \mathbb{Z}_p \backslash p\mathbb{Z}_p$ such that $f(x)$ is a p-adic square?

2. Is there a solution to the simultaneous equations

$$
\left.\begin{aligned}
1 &= \epsilon u_1 + \lambda v_1 + \mu w_1 \\
pz &= \epsilon u_2 + \lambda v_2 + \mu w_2
\end{aligned}\right\}
$$

with z, λ, $\mu \in \mathbb{Z}_p$ and $\epsilon \in \mathbb{Z}_p \backslash p\mathbb{Z}_p$ such that $F(1, pz)$ is a p-adic square?

Let us look at the first question. We can rewrite equation (13) in the form

$$
(14) \qquad \begin{pmatrix} u_1 & v_1 & w_1 & -1 \\ u_2 & v_2 & w_2 & 0 \end{pmatrix} \begin{pmatrix} \epsilon \\ \lambda \\ \mu \\ x \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.
$$

We can solve this using the methods of Section 5. If this does not have a solution, then we cannot answer Question 1 positively and we move on to Question 2. Suppose (14) has a solution. Since $w_2 v_1 - w_1 v_2 \neq 0$, the rank of the matrix in (14) is 2. Thus we can write down ϵ_j, λ_j, μ_j, $x_j \in \mathbb{Z}_p$ for $j = 1, 2, 3$, such that the solutions to (14) are precisely those vectors which can be written in the form

$$
\begin{pmatrix} \epsilon \\ \lambda \\ \mu \\ x \end{pmatrix} = \begin{pmatrix} \epsilon_1 \\ \lambda_1 \\ \mu_1 \\ x_1 \end{pmatrix} + \phi \begin{pmatrix} \epsilon_2 \\ \lambda_2 \\ \mu_2 \\ x_2 \end{pmatrix} + \psi \begin{pmatrix} \epsilon_3 \\ \lambda_3 \\ \mu_3 \\ x_3 \end{pmatrix}
$$

for some ϕ, $\psi \in \mathbb{Z}_p$.

We now proceed as follows. We first write down a finite set $\mathcal{S}$ of "p-adic intervals"; that is, subsets of $\mathbb{Z}_p$ of the form $x_0 + p^s \mathbb{Z}_p$ where $x_0 \in \mathbb{Z}_p$ and $s \geq 0$. We require that $\mathcal{S}$ satisfies the following: x is contained in one of the intervals in $\mathcal{S}$ if and only if there exists ϕ, $\psi \in \mathbb{Z}_p$ such that

- $x = x_1 + \phi x_2 + \psi x_3$,
- $\epsilon_1 + \phi \epsilon_2 + \psi \epsilon_3$ is a p-adic unit.

Once we have $\mathcal{S}$, we know that to answer our question we must check if there exists x in some interval $x_0 + p^s \mathbb{Z}_p$ in $\mathcal{S}$ such that $f(x)$ is a p-adic square. For each interval $x_0 + p^s \mathbb{Z}_p$ in $\mathcal{S}$ we can use Lemma 3.1 to decide if it contains an x for which $f(x)$ is a p-adic square. Thus to answer Question 1 it is now sufficient to write down $\mathcal{S}$.

Let $s = \min(v_p(x_2), v_p(x_3))$. Let $x_2' = x_2/p^s$ and $x_3' = x_3/p^s$. If $x = x_1 + \phi x_2 + \psi x_3$, then $p^s | (x - x_1)$ and $(x - x_1)/p^s = \phi x_2' + \psi x_3'$. Now if p does not divide

$(\epsilon_3 x'_2 - \epsilon_2 x'_3)$ then for any values we wish to give to $(x - x_1)/p^s$ and $\epsilon - \epsilon_1$ we can solve the simultaneous system

$$\begin{aligned} (x - x_1)/p^s &= \phi x'_2 + \psi x'_3, \\ \epsilon - \epsilon_1 &= \phi \epsilon_2 + \psi \epsilon_3, \end{aligned}$$

with ϕ, $\psi \in \mathbb{Z}_p$. Hence in this case $\mathcal{S} = \{x_1 + p^s \mathbb{Z}_p\}$. If however $p | (\epsilon_3 x'_2 - \epsilon_2 x'_3)$, then we can write down ω in $\mathbb{Z}$, such that $\epsilon_i \equiv \omega x'_i \pmod{p}$ for $i = 2$, 3. Thus if $x = x_1 + \phi x_2 + \psi x_3$ and $\epsilon = \epsilon_1 + \phi \epsilon_2 + \psi \epsilon_3$, then $\epsilon - \epsilon_1 \equiv \omega \{(x - x_1)/p^s\}$ $\pmod{p}$. Thus if $p | \omega$ and $p | \epsilon_1$, then $\mathcal{S}$ is empty and we are finished. If p divides ω but not ϵ_1, then $\mathcal{S} = \{x_1 + p^s \mathbb{Z}_p\}$ and we are finished. If p does not divide ω, then we want $(x - x_1)/p^s \not\equiv -\epsilon_1/\omega \pmod{p}$. Let t' be the element of $\{0, 1, \ldots, p - 1\}$ which is congruent to $-\epsilon_1/\omega$ modulo p, and let $T = \{0, 1, \ldots, p - 1\} \setminus \{t'\}$. Then $\mathcal{S} = \{(x_1 + p^s t) + p^{s+1} \mathbb{Z}_p : t \in T\}$.

Question 2 can be decided in a similar manner and can be left for the reader to verify.

Definition. We say that the system of congruences (9) is compatible with the curve (3), if

1. The system has solutions (and thus a parametric solution which we can write down as in Section 6),
2. If it passes the above test.

Otherwise, we say that the system of congruences is not compatible with the curve (3).

The following lemma is trivial.

Lemma 7.1. *With notation as above, given a system of congruences* (9), *we know*

1. *We can test if it is compatible with the curve using the above method.*
2. *If the system of congruences is not compatible with the curve then there is no triple (X, Z, Y) satisfying* (2) *and* (3) *such that (X, Z) satisfies the simultaneous congruences.*

8. The algorithm

Given an interval I such that $f(x)$ is nonnegative for all $x \in I$, and a quadruple $(\alpha, \beta, \gamma, \delta)$ satisfying α, β are coprime, δ is nonzero, γ is square-free and not equal to 0 or 1, and $F(\alpha, \beta) = \gamma \delta^2$.

Notation. Let B, N, ζ be as in Theorem 2.4. Define

$$\mathcal{G}(\alpha, \beta, I) = \{(\zeta P h, P N) \mid P \in B, h \in H\}.$$

We now restate the main result of Section 2.

Theorem 8.1. *Let I be an interval in $\mathbb{R}$ such that $f(x)$ is nonnegative for all $x \in I$. Suppose $(\alpha, \beta, \gamma, \delta)$ is a quadruple of integers satisfying the conditions above, and let $\mathcal{G}(\alpha, \beta, I)$ be as above. If (X, Z, Y) satisfies* (2) *and* (3), *then there exists a pair (u, M) in $\mathcal{G}(\alpha, \beta, I)$ such that $\beta X - \alpha Z \equiv u \pmod{M}$.*

Proof. This is simply a restatement of Theorem 2.4. □

Suppose now that we are given an interval I such that $f(x)$ is nonnegative for all $x \in I$, and a set of quadruples $(\alpha_i, \beta_i, \gamma_i, \delta_i)$, $i = 1, \ldots, m$, each satisfying the usual conditions: α_i, β_i are coprime, $F(\alpha_i, \beta_i) = \gamma_i \delta_i^2$, δ_i is nonzero, and γ_i is

square-free and is neither 0 nor 1. We have by the above theorem, for each i, a finite set of pairs $\mathcal{G}_i = \mathcal{G}(\alpha_i, \beta_i, I)$, such that if (X, Z, Y) satisfies (2) and (3), then for each i, $\beta_i X - \alpha_i Z \equiv u \pmod{M}$ for some pair $(u, M) \in \mathcal{G}_i$.

Now for each i we can fix a pair $(u_i, M_i) \in \mathcal{G}_i$ and ask if there exists some (X, Z, Y) satisfying (2) and (3) such that

$$(15) \qquad \beta_i X - \alpha_i Z \equiv u_i \pmod{M_i}$$

for $i = 1, \ldots, m$. We do not know of a way which will always answer this question. Rather we can attempt to show that the congruences are inconsistent: that is, we can apply the method of Section 7 to test if the system of congruences is compatible with the curve (3) (this term is explained at the end of Section 7). If it is not, then the answer is clearly no. If it is compatible with the curve, then while performing that test we will have parametrized the solutions to the simultaneous congruences (15); we will have written down a triple of vectors $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w} \in \mathbb{Z}^2$ such that any solution to the simultaneous congruences is of the form

$$(16) \qquad \begin{pmatrix} X \\ Z \end{pmatrix} = \mathbf{u} + \lambda \mathbf{v} + \mu \mathbf{w}$$

for some λ, $\mu \in \mathbb{Z}$. We can then try small values of λ, $\mu \in \mathbb{Z}$ and ask if these give a pair X, Z such that $F(X, Z)$ is a square in $\mathbb{Z}$.

If we find that for each possible combination of the $(u_i, M_i) \in \mathcal{G}_i$ the system of congruences (15) is not compatible with the curve, then it is clear that there are no triples (X, Z, Y) satisfying (2) and (3). That this can happen is illustrated by our example in Section 4.

If we are to follow this strategy, then we will have to look at $d_1 \times d_2 \times \cdots \times d_m$ systems of simultaneous congruences, where d_i is the size of $\mathcal{G}_i$. This number can be enormous. In practice we aim to choose our quadruples $(\alpha_i, \beta_i, \gamma_i, \delta_i)$ in such a way that many of the γ's have common factors. Now for each i, the integer γ_i divides every M of every pair (u, M) in $\mathcal{G}_i$. We rearrange the quadruples so that, as often as possible, several consecutive γ's have a common factor. We then do what is called a "depth-first search". Given a set of quadruples $(\alpha_i, \beta_i, \gamma_i, \delta_i)$, $i = 1, \ldots, m$, and the corresponding $\mathcal{G}_i$, the algorithm below (which we write in pseudo-code) produces a set of triples $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w} \in \mathbb{Z}^2$. The algorithm is designed so that such a triple is in the output if and only if for some choice of $(u_1, M_1) \in \mathcal{G}_1, \ldots, (u_m, G_m) \in \mathcal{G}_m$, the system (15) is compatible with (3), and this triple gives a parametric solution to the system of congruences.

In the algorithm we think of $\mathcal{G}_i$ as an ordered list of pairs. Thus it makes sense to speak of the FIRST_PAIR$(\mathcal{G}_i)$, and the LAST_PAIR$(\mathcal{G}_i)$. If (u, M) is in $\mathcal{G}_i$ but is not the last pair, then we let the one after it be NEXT_PAIR$(\mathcal{G}_i, (u, M))$. In the algorithm L is a sequence of pairs $[(u_i, M_i) : i = 1, \ldots, r]$, where always $r = \text{LENGTH}(L)$ is at most $\leq m$, the number of our $\mathcal{G}_i$. We always have that each (u_i, M_i) is an element of $\mathcal{G}_i$ for $i = 1, \ldots, r$. Further APPEND$(L, (u, M))$ appends the pair (u, M) to end of L.

TEST(L) means test the system of congruences $\beta_i X - \alpha_i Z \equiv u_i \pmod{M_i}$ with $i = 1, \ldots, r$ for compatibility with the curve (3). If it is not compatible with the curve then TEST$(L) = 0$, and otherwise TEST$(L) = [\mathbf{u}, \mathbf{v}, \mathbf{w}]$, where $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$ parametrize the solutions to the congruences in the usual way.

```
INPUT: Interval I, quadruples (α_i, β_i, γ_i, δ_i), and G_i, i = 1,..., m.
OUTPUT: A set of triples u, v, w ∈ Z² (see Theorem 8.2 below).
```
1. BEGIN
2. $L = [\text{FIRST\_PAIR}(\mathcal{G}_1)]$;
3. $T = \text{TEST}(L)$; IF $T = 0$ GO TO STEP 5;
4. IF LENGTH(L) $< m$ THEN $L = \text{APPEND}(L, \text{FIRST\_PAIR}(\mathcal{G}_{r+1}))$ AND GO TO STEP 3 OTHERWISE OUTPUT T;
(*Compute the largest i such that* $L[i] \neq \text{LAST\_PAIR}(\mathcal{G}_i)$ *and let this be s*)
5. $s = m$; $f = 1$;
6. WHILE $s \geq 0$ AND $f = 1$ DO
7.   IF $L[s] \neq \text{LAST\_PAIR}(\mathcal{G}_s)$ THEN $f = 0$ OTHERWISE $s = s - 1$ OD;
8. IF $s = m$ THEN END;
9. $L[s] = \text{NEXT\_PAIR}(\mathcal{G}_s, L[s])$; $L = [L[i] \ : \ i = 1, \ldots, s]$;
10. GO TO STEP 3;

Theorem 8.2. *Given an interval I such that $f(x) \geq 0$ for all $x \in I$, quadruples $(\alpha_i, \beta_i, \gamma_i, \delta_i)$ $(i = 1, \ldots, m)$ satisfying the usual conditions, and the corresponding $\mathcal{G}_i$, the above algorithm produces a finite set of triples of vectors $[\mathbf{u}, \mathbf{v}, \mathbf{w}]$ (with $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w} \in \mathbb{Z}^2$) subject to the following condition: a triple is in the output if and only if there exists $(u_1, M_1) \in \mathcal{G}_1, \ldots, (u_m, M_m) \in \mathcal{G}_m$ such that the system of congruences (15) is compatible with the curve (3), and $[\mathbf{u}, \mathbf{v}, \mathbf{w}]$ give a parametric solution to the congruences.*

In particular, if there exists (X, Z, Y) satisfying (2) and (3) then X, Z satisfies equation (16) for some integers λ, μ, and some triple in the output $[\mathbf{u}, \mathbf{v}, \mathbf{w}]$. If the algorithm does not give any output, then there are no triples (X, Z, Y) satisfying (2) and (3).

Proof. Suppose for now that the first statement of the theorem holds. If (X, Z, Y) satisfies (2) and (3), then by Theorem 8.1, there exists for each i a pair $(u_i, M_i) \in \mathcal{G}_i$ such that the simultaneous congruences (15) hold. Then these congruences have a global solution on the curve and thus are compatible with it. Now the second part of the theorem follows from the first.

Let us now come to the first statement. Consider a directed graph where the vertices are the elements of $\mathcal{G}_i$ for $i = 1, \ldots, m$, and where vertices (u, M), (u', M') are connected by an arrow $(u, M) \to (u'', M'')$ if and only if there is some $1 \leq i \leq m - 1$ such that $(u, M) \in \mathcal{G}_i$ and $(u', M') \in \mathcal{G}_{i+1}$. We write $[(u_1, M_1), \ldots, (u_r, M_r)]$ for the path which starts with $(u_1, M_1) \in \mathcal{G}_1$ and finishes in $(u_r, M_r) \in \mathcal{G}_r$. What we want in effect is for our algorithm to determine all paths $[(u_1, M_1), \ldots, (u_m, M_m)]$ such that the corresponding system (15) is compatible with the curve (3). Now we observe that if, for some $r < m$, the system of congruences corresponding to the path $[(u_1, M_1), \ldots, (u_r, M_r)]$ is not compatible with the curve, then neither is any extension of it $[(u_1, M_1), \ldots, (u_r, M_r), (u_{r+1}, M_{r+1}), \ldots, (u_m, M_m)]$ for any elements $(u_j, M_j) \in \mathcal{G}_j$ with $j = r + 1, \ldots, m$.

What is now needed is merely to carry out a "depth-first search" of a directed graph (see for example [AHU]) and it can safely be left for the reader to see that our algorithm does exactly that (bearing in mind that the algorithm L records the current path). □

The above algorithm minimizes the storage requirement. Essentially the only storage is the input and final output. Also the fact that we choose and rearrange our input so that successive γ's often have common factors probably greatly reduces the running time. To see this, suppose say that γ_1 and γ_2 have the common factor $l > 1$. Suppose in the above algorithm that $L = [(u_1, M_1), (u_2, M_2)]$ is given. Here we must have that $(u_i, M_i) \in \mathcal{G}_i$ for $i = 1,\ 2$. Then $M_1,\ M_2$ have l as a common factor. It is then fairly likely that for each prime p dividing l, the simultaneous pair of congruences (15) with $i = 1,\ 2$ will have exactly one solution, say $x,\ z$ modulo that p. We expect that roughly 50 percent of the time $F(x, z)$ is not a square modulo p, and that even if it is, our solution modulo p does not necessarily lift to give us a p-adic point on $\mathbb{P}C(\mathbb{Z}_p)$. Thus when running our algorithm, we have a good chance of not having to go any deeper at this stage and we simply replace (u_2, M_2) with the next pair in $\mathcal{G}_2$ (or if (u_2, M_2) is the last pair in $\mathcal{G}_2$, then we replace (u_1, M_1) by the next pair in $\mathcal{G}_1$ and we let $L = [(u_1, M_1)]$).

9. A second example

If our algorithm fails to prove the nonexistence of rational points on our hyperelliptic curve, or if indeed the curve does have rational points, then it may still be useful to search for all rational points whose height is less than a certain given bound. It is the purpose of this example to illustrate how the output from the algorithm of the previous section may be used to speed up this search.

Consider the curve

$$y^2 = x^3 - 1063395x - 422075394$$

of conductor 3672. This curve comes from Cremona's extended tables of elliptic curves available via the World Wide Web from: `http://www.nott.ac.uk/perso-nal/jec/ftp/data`. The conjecture of Birch and Swinnerton-Dyer predicts that it has rank 1, and we content ourselves with finding one point of infinite order on the curve. Cremona's `mwrank` gives the following 2-covering:

$$Y^2 = -216X^4 + 252X^3Z - 315X^2Z^2 - 1476XZ^3 - 762Z^4.$$

We define $f(x)$ and $F(X, Z)$ as usual. Note that $f(x)$ is nonnegative if and only if $x \in I$, where $I = [-0.81295674, -0.81294900]$ (we have rounded the end-points of the interval to eight decimal places). We did a search for quadruples $\alpha,\ \beta,\ \gamma,\ \delta$ as in the example in Section 4 but this time with range $-200 \le \alpha \le 200$ and $0 \le \beta \le 200$. We found the following values.

α	β	γ	δ
-113	139	3	1
-13	16	-6	2
-5	6	-3	18
1	0	-6	6

As stated previously, we implemented all the algorithms in this paper in `pari/GP`. Our main algorithm of Section 8 took 4.5 seconds to run and gave 4 triples $[\mathbf{u}, \mathbf{v}, \mathbf{w}]$, which we give here as triples of row vectors:

$$[(421, 6), (36, 0), (24, 144)], \quad [(23, 66), (36, 0), (24, 144)],$$
$$[(1273, 6), (108, 0), (96, 144)], \quad [(71, 66), (108, 0), (96, 144)].$$

In the notation of Lemma 6.1, the quantities $|w_2v_1 - w_1v_2|$ are 432, 432, 1296, 1296, respectively. To get an idea of just how efficient our sieve is, we note that

given (say) a very large square in $\mathbb{R}^2$, the proportion of $(X, Z) \in \mathbb{Z}^2$ in our square which can be expressed in the form $\mathbf{u} + \lambda\mathbf{v} + \mu\mathbf{w}$ for some integral λ, μ, where $[\mathbf{u}, \mathbf{v}, \mathbf{w}]$ is one of our four triples is roughly $2/432 + 2/1296 = 1/162$. In fact using these four triples, it took our program roughly 4 minutes to search the region

$$-10^7 \leq X \leq 10^7, \ 1 \leq Z \leq 10^7,$$

and to find one point $(X, Z, Y) = (-2021077, 2486082, 168298146)$ on our 2-covering; here

$$(X, Z) = \mathbf{u} - 67651\mathbf{v} + 17264\mathbf{w},$$

where $[\mathbf{u}, \mathbf{v}, \mathbf{w}]$ is the second triple given above. Using the standard syzygy in Section 3.6 of [Cre1] we get the point

$$\left[\frac{5580280211292650758}{87420573910609}, \frac{1318035111718925835621378626}{817373361745081357273} \right]$$

on our original elliptic curve. By contrast, a program written by Cremona based on more usual sieving ideas (as described in Section 3.6 of of [Cre1]) and running on the same machine, took roughly 95 minutes to find the point on the 2-covering.

We point out that there are other methods/programs which can be used to compute the generator above. For example, there is an (unpublished) experimental method due to Cremona and Silverman ([Cre2]) for curves of rank 1 using Heegner points and canonical heights. We would like to thank J. Cremona for running his implementation of this method on the above example. The program, running on a 90MHZ Pentium, took just 79 seconds to find the point on the elliptic curve.

References

[AHU]   A. V. Aho, J. E. Hopcroft, J. D. Ullman, *Data Structures and Algorithms*, Addison-Wesley, 1982. MR **84f:**68001

[Cal]   J. W. S. Cassels, *Local Fields*, LMS Student Texts, Cambridge University Press, 1986. MR **87i:**11172

[Ca2]   J. W. S. Cassels, *Survey Article: Diophantine Equations with Special Reference to Elliptic Curves*, J.L.M.S. *41* (1966), 193-291. MR **33:**7299

[Ca3]   J. W. S. Cassels, *Second Descents for Elliptic Curves*, J. reine angew. Math. **494** (1998), 101–127. MR **99d:**11058

[Cohen] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM 138, Springer-Verlag, third corrected printing, 1996. MR **94i:**11105

[Cohn]   P. M. Cohn, *Algebra, Volume I*, second edition, John Wiley and Sons, 1982. MR **83e:**00002

[Cre1]   J. E. Cremona, *Algorithms for Modular Elliptic Curves*, second edition, Cambridge University Press, 1997. MR **99e:**11068

[Cre2]   J. E. Cremona, *Personal Communication*, 1996.

[Me,Si,Sm] J.R. Merriman, S. Siksek and N.P. Smart, *Explicit 4-Descents on an Elliptic Curve*, Acta Arith. **LXXVII** (1996), 385-404. MR **97j:**11027

[Sil]   J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, 1986. MR **87g:**11070

Institute of Mathematics and Statistics, Cornwallis Building, University of Kent, Canterbury, UK

Current address: Department of Mathematics, College of Science, PO Box 36, Sultan Qaboos University, Oman

E-mail address: siksek@squ.edu.om