# Topics in Diophantine Equations

**Sir Peter Swinnerton-Dyer**

## 1 Introduction

These notes fall into two parts. The first part, which goes up to the end of Sect. 5, is a general survey of some of the topics in the theory of Diophantine equations which interest me and on which I hope to see progress within the next 10 years. Because of the second condition, I have for example not covered the Riemann Hypothesis or the Birch/Swinnerton-Dyer conjectures, both of which at the moment appear intractable. Another such survey can be found in Silverberg [1]; it has little overlap with this one but should appeal to the same readers. In the second part of these notes, I go into more detail on some particular topics than there was time for in the lectures.

A *Diophantine problem* over **Q** or **Z** is concerned with the solutions either in **Q** or in **Z** of a finite system of polynomial equations

$$F_i(X_1, \ldots, X_n) = 0 \quad (1 \le i \le m) \tag{1}$$

with coefficients in **Q**. Without loss of generality we can obviously require the coefficients to be in **Z**. A system (1) is also called a system of *Diophantine equations*. Often one will be interested in a family of such problems rather than a single one; in this case one requires the coefficients of the $F_i$ to lie in some $\mathbf{Q}(c_1, \ldots, c_r)$, and one obtains an individual problem by giving the $c_j$ values in **Q**. Again one can get rid of denominators. Some of the most obvious questions to ask about such a family are:

(A) Is there an algorithm which will determine, for each assigned set of values of the $c_j$, whether the corresponding Diophantine problem has solutions, either in **Z** or in **Q**?

(B) When the answer to (A) is positive, is there for values of the $c_j$ for which the system is soluble an algorithm for exhibiting a solution? For example, is there

Sir P. Swinnerton-Dyer (✉)

Department of Pure Mathematics and Mathematical Statistics, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WB, UK

e-mail: H.P.F.Swinnerton-Dyer@dpmms.cam.ac.uk

an upper bound for the height of the smallest solution in terms of the heights of the coefficients of (1)?

For individual members of such a family, it is also natural to ask:

(C)    Can we describe the set of all solutions, or even its structure?
(D)    Is the phrase "density of solutions" meaningful, and if so, what can we say about it?

The attempts to answer these questions have led to the introduction of new ideas and these have generated new questions. Progress in mathematics usually comes by proving results; but sometimes a well justified conjecture throws new light on the structure of the subject. (For similar reasons, well motivated computations can be helpful; but computations not based on a feeling for the structure of the subject have generally turned out to be a waste of time.)

Though the problems associated with solutions in $\mathbf{Z}$ and in $\mathbf{Q}$ may look very similar (and indeed were believed for a long time to be so), it now appears that the methods which are useful are actually very different; and currently the theory for solutions in $\mathbf{Q}$ has much more structure than that for solutions in $\mathbf{Z}$. The main reason for this seems to be that in the rational case the system (1) defines a variety in the sense of algebraic geometry, and many of the tools of that discipline can be used. Despite the advent of Arakelov geometry, this is much less true of integral problems. However, for most families of varieties of degree greater than 2 it is only in low dimension that we yet know enough of the geometry for it to be useful. Uniquely, the Hardy-Littlewood method is useful both for integral and for rational problems; it was designed for integral problems but it can also be applied to rational problems by making the equations homogeneous. There is a brief discussion of this method in Sect. 5 and a comprehensive survey in [2].

Denote by $V$ the variety defined by (1) and let $V'$ be any variety birationally equivalent to $V$ over $\mathbf{Q}$. Rational solutions of (1) in $\mathbf{Q}$ are just rational points on $V$, and finding them is almost the same as finding rational points on $V'$. Hence (except for Question (D) above) one expects the properties of the rational solutions of (1) to be essentially determined by the birational equivalence class of $V$ over $\mathbf{Q}$. Classifying Diophantine problems over $\mathbf{Q}$ therefore corresponds to classifying birational equivalence classes of varieties over $\mathbf{Q}$. A first crude approximation to this is to classify them over $\mathbf{C}$. So number theorists would be helped if geometers could develop an adequate classification of varieties. At the moment, such a classification is reasonably complete for curves and surfaces, but it is still fragmentary even in dimension 3; so for those number theorists who use geometric methods it is natural to concentrate on curves and surfaces and on certain particularly simple kinds of variety of higher dimension.

The definitions and the questions above can be generalized to an arbitrary algebraic number field and the ring of integers in it; the answers are usually known or conjectured to be similar to those over $\mathbf{Q}$ or $\mathbf{Z}$, though the proofs can be very much harder. (But there are exceptions; for example, the modularity of elliptic curves only holds over $\mathbf{Q}$.) Some of the questions above can also be posed for other fields of number-theoretic interest – in particular for finite fields and for completions of

algebraic number fields – and when one studies Diophantine problems it is often essential to consider these fields also. If $V$ is defined over a field $K$, the set of points on $V$ defined over $K$ is denoted by $V(K)$. If $V(K)$ is not empty we say that $V$ is *soluble in $K$*. In the special case where $K = k_v$, the completion of an algebraic number field $k$ at the place $v$, we also say that $V$ is *locally soluble at $v$*. From now on we denote by $\mathbf{Q}_v$ any completion of $\mathbf{Q}$; thus $\mathbf{Q}_v$ means $\mathbf{R}$ or some $\mathbf{Q}_p$.

One major reason for considering solubility in complete fields and in finite fields is that a necessary condition for (1) to be soluble in $\mathbf{Q}$ is that it is soluble in every $\mathbf{Q}_v$. The condition of solubility in every $\mathbf{Q}_v$ is computationally decidable; see Sect. 2. Moreover the first step in deciding solubility in $\mathbf{Q}_p$ is to study the solutions of the system reduced mod $p$ in the finite field $\mathbf{F}_p$ of $p$ elements.

Diophantine problems were first introduced by Diophantus of Alexandria, the last of the great Greek mathematicians, who lived at some time between 300 BC and 300 AD; but he was handicapped by having only one letter available to represent variables, all the others being used in the classical world to represent specific numbers. Individual Diophantine problems were studied by such great mathematicians as Fermat, Euler and Gauss. But it was Hilbert's address to the International Congress in 1900 which started the development of a systematic theory. His tenth problem asked:

> Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: to devise a process according to which it can be determined by a finite number of operations whether the equation is soluble in rational integers.

Most of the early work on Diophantine equations was concerned with rational rather than integral solutions; presumably Hilbert posed this problem in terms of integral solutions because such a process for integral solutions would automatically provide the corresponding process for rational solutions also. In the confident days before the First World War, it was assumed that such a process must exist; but in 1970 Matijasevič showed that this was impossible. He exhibited a polynomial $F(c; x_1, \ldots, x_n)$ such that there cannot exist an algorithm which will decide for every given integer $c$ whether $F = 0$ is soluble in integers. His proof is part of the great program on decidability initiated by Gödel; good accounts of it can be found in [3], pp 323–378 or [4]. The corresponding question for rational solutions is still open; I am among the few who believe that it may have a positive answer. Certainly it is important to ask for which families of varieties such a process exists, and to find such a process when it does exist.

## 2  The Hasse Principle and the Brauer-Manin Obstruction

Let $V$ be a variety defined over $\mathbf{Q}$. If $V$ is locally soluble at every place of $\mathbf{Q}$, we say that it satisfies the *Hasse condition*. If $V(\mathbf{Q})$ is not empty then $V$ certainly satisfies the Hasse condition, so the latter is necessary for solubility. What makes this remark

valuable is that the Hasse condition is computable – that is, one can decide in finitely many steps whether a given $V$ satisfies the Hasse condition. This follows from the next two lemmas.

**Lemma 2.1.** *Let $W$ be an absolutely irreducible variety of dimension $n$ defined over the finite field $k = \mathbf{F}_p$. Then $N(p)$, the number of points on $W$ defined over $k$, satisfies*

$$|N(p) - p^n| < Cp^{n-1/2}$$

*where the constant $C$ depends only on the degree and dimension of $W$ and is computable.*

This follows from the Weil conjectures, for which see Sect. 3; but weaker results which are adequate for the proof that the Hasse condition is computable were known much earlier. Since the singular points of $W$ lie on a proper subvariety, there are at most $C_1 p^{n-1}$ of them, where $C_1$ is also computable. It follows that if $p$ exceeds a computable bound depending only on the degree and dimension of $W$ then $W$ contains a nonsingular point defined over $\mathbf{F}_p$.

Let $V$ be an absolutely irreducible nonsingular variety defined over $\mathbf{Q}$, embedded in affine or projective space. We obtain $\tilde{V}_p$, its reduction mod $p$, by taking all the equations for $V$ with coefficients in $\mathbf{Z}$ and mapping the coefficients into $\mathbf{F}_p$. If $\tilde{V}_p$ is nonsingular and has the same dimension as $V$, then $V$ is said to have *good reduction* at $p$; this happens for all but a finite computable set of primes $p$. If $p$ is large enough, it follows from the remarks above that $\tilde{V}_p$ contains a nonsingular point $Q_p$ defined over $\mathbf{F}_p$. The result which follows, which is known as Hensel's Lemma though the idea of the proof goes back to Newton, now shows that $V$ contains a point $P_p$ defined over $\mathbf{Q}_p$.

**Lemma 2.2.** *Let $V$ be an absolutely irreducible variety defined over $\mathbf{Q}$ which has a good reduction $\tilde{V}_p$ mod $p$. If $\tilde{V}_p$ contains a nonsingular point $Q_p$ defined over $\mathbf{F}_p$ then $V$ contains a nonsingular point $P_p$ defined over $\mathbf{Q}_p$ whose reduction mod $p$ is $Q_p$.*

In view of this, to decide whether $V$ satisfies the Hasse condition one only has to check solubility in $\mathbf{R}$ and in finitely many $\mathbf{Q}_p$. Each of these checks can be shown to be a finite process.

A family $\mathscr{F}$ of varieties is said to satisfy the *Hasse Principle* if every $V$ contained in $\mathscr{F}$ and defined over $\mathbf{Q}$ which satisfies the Hasse condition actually contains at least one point defined over $\mathbf{Q}$. Again, a family $\mathscr{F}$ is said to admit *weak approximation* if every $V$ contained in $\mathscr{F}$ and defined over $\mathbf{Q}$, and such that $V(\mathbf{Q})$ is not empty, has the following property: given any finite set of places $v$ and corresponding non-empty sets $\mathscr{N}_v \subset V(\mathbf{Q}_v)$ open in the $v$-adic topology, there is a point $P$ in $V(\mathbf{Q})$ which lies in each of the $\mathscr{N}_v$. In the special case when $\mathscr{F}$ consists of a single variety $V$, and $V(\mathbf{Q})$ is not empty, we simply say that $V$ admits weak approximation. Whether $V$ admits weak approximation appears not to be computable in general; for a case where it is, see [5]. All this generalizes effortlessly to an arbitrary algebraic number field.

The most important families which are known to have either of these properties (and which actually have both) are the families of quadrics of any given dimension; this was proved by Minkowski for quadrics over $\mathbf{Q}$ and by Hasse for quadrics over an arbitrary algebraic number field. They also both hold for Severi-Brauer varieties, which are varieties biregularly equivalent to some $\mathbf{P}^n$ over $\mathbf{C}$. But many families, even of very simple varieties, do not satisfy either the Hasse Principle or weak approximation. (For example, neither of them holds for nonsingular cubic surfaces.) It is therefore natural to ask

*Question 2.3.* For a given family $\mathscr{F}$, what are the obstructions to the Hasse Principle and to weak approximation?

For weak approximation there is a variant of this question which may be more interesting and and is certainly easier to answer. For another way of stating weak approximation on $V$ is to say that if $V(\mathbf{Q})$ is not empty then it is dense in the adelic space $V(\mathbf{A}) = \prod_v V(\mathbf{Q}_v)$. This suggests the following:

*Question 2.4.* For a given $V$, or family $\mathscr{F}$, what can be said about the closure of $V(\mathbf{Q})$ in the adelic space $V(\mathbf{A})$?

For the example of cubic surfaces, see [5]. However, there are families for which Question 2.3 does not seem to be a sensible question to ask; these probably include for example all families of varieties of general type. So one should also back up Question 2.3 with

*Question 2.5.* For what kinds of families is either part of Question 2.3 a sensible question to ask?

The only known systematic obstruction to the Hasse Principle or to weak approximation is the Brauer-Manin obstruction, though obstructions can be found in the literature which are not Brauer-Manin. (See for example Skorobogatov [6].) It is defined as follows. Let $A$ be a *central simple algebra* – that is, a simple algebra which is finite dimensional over a field $K$ which is its centre. Each such algebra consists, for fixed $D$ and $n$, of all $n \times n$ matrices with elements in a division algebra $D$ with centre $K$. Two central simple algebras over $K$ are *equivalent* if they have the same underlying division algebra. Formation of tensor products over $K$ gives the set of equivalence classes the structure of a commutative group, called the *Brauer group* of $K$ and written $\mathrm{Br}(K)$. There is a canonical isomorphism $\iota_p : \mathrm{Br}(\mathbf{Q}_p) \simeq \mathbf{Q}/\mathbf{Z}$ for each $p$; and there is a canonical isomorphism $\iota_\infty : \mathrm{Br}(\mathbf{R}) \simeq \{0, \frac{1}{2}\}$, the nontrivial division algebra over $\mathbf{R}$ being the classical quaternions.

Let $B$ be an element of $\mathrm{Br}(\mathbf{Q})$. Tensoring $B$ with any $\mathbf{Q}_v$ gives rise to an element of $\mathrm{Br}(\mathbf{Q}_v)$, and this element is trivial for almost all $v$. There is an exact sequence

$$0 \to \mathrm{Br}(\mathbf{Q}) \to \bigoplus \mathrm{Br}(\mathbf{Q}_v) \to \mathbf{Q}/\mathbf{Z} \to 0,$$

due to Hasse, in which the third map is the sum of the $\iota_v$; it tells us when a set of elements, one in each $\mathrm{Br}(\mathbf{Q}_v)$ and almost all trivial, can be generated from some element of $\mathrm{Br}(\mathbf{Q})$.

Now let $V$ be a complete nonsingular variety defined over $\mathbf{Q}$ and $A$ an *Azumaya algebra* on $V$ – that is, a simple algebra with centre $\mathbf{Q}(V)$ which has a good specialization at every point of $V$. The group of equivalence classes of Azumaya algebras on $V$ is denoted by $\mathrm{Br}(V)$. If $P$ is any point of $V$, with field of definition $\mathbf{Q}(P)$, we obtain a simple algebra $A(P)$ with centre $\mathbf{Q}(P)$ by specializing at $P$. For all but finitely many $p$, we have $\iota_p(A(P_p)) = 0$ for all $p$-adic points $P_p$ on $V$. Thus, as was first noticed by Manin, a necessary condition for the existence of a rational point $P$ on $V$ is that for every $v$ there should be a $v$-adic point $P_v$ on $V$ such that

$$\sum \iota_v(A(P_v)) = 0 \quad \text{for all } A. \tag{2}$$

Similarly, a necessary condition for $V$ with $V(\mathbf{Q})$ not empty to admit weak approximation is that (2) should hold for all Azumaya algebras $A$ and all adelic points $\prod_v P_v$. In each case this is the *Brauer-Manin condition*. It is clearly unaffected if we add to $A$ a constant algebra – that is, an element of $\mathrm{Br}(\mathbf{Q})$. So what we are really interested in is $\mathrm{Br}(V)/\mathrm{Br}(\mathbf{Q})$.

All this can be put into highbrow language. For any $V$ there is an injection of $\mathrm{Br}(V)$ into the étale cohomology group $\mathrm{H}^2(V, \mathbf{G}_m)$; and if for example $V$ is a complete nonsingular surface, this injection is an isomorphism. If we write

$$\mathrm{Br}_1(V) = \ker(\mathrm{Br}(V) \to \mathrm{Br}(\bar{V})) = \ker(\mathrm{H}^2(V, \mathbf{G}_m) \to \mathrm{H}^2(\bar{V}, \mathbf{G}_m)),$$

there is a filtration

$$\mathrm{Br}(\mathbf{Q}) \subset \mathrm{Br}_1(V) \subset \mathrm{Br}(V).$$

However, not even the abstract structure of $\mathrm{Br}(V)/\mathrm{Br}_1(V)$ is known; and there is no known systematic way of finding Azumaya algebras which represent nontrivial elements of this quotient, though in a particular case Harari [7] has exhibited a Brauer-Manin obstruction coming from such an algebra. In contrast, provided the Picard variety of $V$ is trivial there is an isomorphism

$$\mathrm{Br}_1(V)/\mathrm{Br}(\mathbf{Q}) \simeq \mathrm{H}^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), \mathrm{Pic}(V \otimes \bar{\mathbf{Q}})),$$

and this is computable in both directions provided the Néron-Severi group of $V$ over $\bar{\mathbf{Q}}$ is known and is torsion-free. (For details of this, see [8].)

There is no known systematic way of determining the Néron-Severi group for arbitrary $V$, and there is strong reason to suppose that this is really a number-theoretic rather than a geometric problem. One may need to approach this question through the Tate conjectures, for which see Sect. 3; but this is a very long-term strategy. However, it is usually possible to determine it for any given $V$, even if one cannot prove that this determination is correct.

*Question 2.6.* Is there a general algorithm (even conjectural) for determining the Néron-Severi group of $V$ for varieties $V$ defined over an algebraic number field?

Lang has conjectured that if $V$ is a variety of general type defined over an algebraic number field $K$ then there is a finite union $\mathscr{S}$ of proper subvarieties of $V$ such

that every point of $V(K)$ lies in $\mathscr{S}$. (Faltings' theorem, for which see Sect. 4, is the special case of this for curves.) This raises another question, similar to Question 2.6 but probably somewhat easier:

*Question 2.7.* Is there an algorithm for determining $\text{Pic}(V)$ where $V$ is a variety defined over an algebraic number field?

The Brauer-Manin obstruction was introduced by Manin [9] in order to bring within a single framework various sporadic counterexamples to the Hasse principle. The theory of this obstruction has been extensively developed, largely by Colliot-Thélène and Sansuc. In particular, for rational varieties they have shown how to go back and forth between the Brauer-Manin condition and the descent condition for torsors under tori. They also defined universal torsors and showed that if there is no Brauer-Manin obstruction to the Hasse principle on a variety $V$ then there exists a universal torsor over $V$ which has points everywhere locally. This suggests that one should pay particular attention to Diophantine problems on universal torsors. Unfortunately, it is usually not easy to exploit what is known about the geometric structure of universal torsors. Indeed there are very few families for which the Brauer-Manin obstruction can be nontrivial but for which it has been shown that it is the only obstruction to the Hasse principle. (See however [10] and, subject to Schinzel's hypothesis, [11, 12].) Colliot-Thélène and Sansuc have conjectured that the Brauer-Manin obstruction is the only obstruction to the Hasse principle for rational surfaces – that is, surfaces birationally equivalent to $\mathbf{P}^2$ over $\bar{\mathbf{Q}}$. On the other hand, Skorobogatov ([6], and see also [13]) has exhibited on a bielliptic surface an obstruction to the Hasse principle which is definitely not Brauer-Manin.

*Question 2.8.* Is the Brauer-Manin obstruction the only obstruction to the Hasse principle for all unirational (or all Fano) varieties?

For the method of universal torsors, the immediate question to address must be the following:

*Question 2.9.* Does the Hasse principle hold for universal torsors over a rational surface?

We can of course ask similar questions for weak approximation. Both for the Hasse principle and for weak approximation one can alternatively ask what is the most general class of varieties for which the Brauer-Manin obstruction is the only one. Colliot-Thélène has suggested that this class probably includes all rationally connected varieties.

There are families $\mathscr{F}$ whose universal torsors appear to be too complicated to be systematically investigated, but for which it is still possible to identify the obstruction to the Hasse principle. It is sometimes possible to start from the absence of a Brauer-Manin obstruction (the most impressive example being Chap. 3 of Wittenberg [14]); but there are also alternative strategies. Implementing these falls naturally into two parts:

1. Assuming that $V$ in $\mathscr{F}$ satisfies the Hasse condition, one finds a necessary and sufficient condition for $V$ to have a rational point, or to admit weak approximation.

2. One then shows that this necessary and sufficient condition is equivalent to the Brauer-Manin condition.

Both parts of this strategy have been applied to pencils of conics, where one uses Schinzel's Hypothesis to implement (1); see [12, 11]. Except for Skorobogatov's example above, I know of no families for which it has been possible to carry out (1) but not (2). But there are families for which it has been possible to find a sufficient condition for solubility (additional to the Hasse condition) which appears rather weak but which is definitely stronger than the Brauer-Manin condition. The obvious examples of such a condition are the various forms of what is called Conditions D or E in [15, 16, 17, 18]. However, in these cases it is not obvious that a condition stronger than the Brauer-Manin condition is actually necessary; and I attribute the gap to clumsiness in the proofs.

*Question 2.10.* When the Brauer-Manin condition is trivial, how can one make use of this fact?

In addition to the work of Wittenberg cited above, there are at least two known approaches to this question: by descent using torsors, and by the fibration method exploited in particular by Harari.

## 3 Zeta-Functions and L-Series

Let $W \subset \mathbf{P}^n$ be a nonsingular and absolutely irreducible projective variety of dimension $d$ defined over the finite field $k = \mathbf{F}_q$, and denote by $\phi(q)$ the Frobenius automorphism of $W$ given by

$$\phi(q) : (x_0, x_1, \ldots, x_n) \mapsto (x_0^q, x_1^q, \ldots, x_n^q).$$

For any $r > 0$ the fixed points of $(\phi(q))^r$ are precisely the points of $W$ which are defined over $\mathbf{F}_{q^r}$; suppose that there are $N(q^r)$ of them. Although the context is totally different, this is almost the formalism of the Lefschetz Fixed Point theorem, since for geometric reasons each of these fixed points has multiplicity $+1$. This analogy led Weil to conjecture that there should be a cohomology theory applicable in this context. This would imply that there were finitely many complex numbers $\alpha_{ij}$ such that

$$N(q^r) = \sum_{i=0}^{2d} \sum_{j=1}^{B_i} (-1)^i \alpha_{ij}^r \quad \text{for all } r > 0, \tag{3}$$

where $B_i$ is the dimension of the $i$th cohomology group of $W$ and the $\alpha_{ij}$ are the characteristic roots of the map induced by $\phi(q)$ on the $i$th cohomology. For each $i$ duality asserts that $B_i = B_{2d-i}$ and the $\alpha_{2d-i,j}$ are a permutation of the $q^d/\alpha_{ij}$. If we define the local zeta-function $Z(t, W)$ by either of the equivalent relations

$$\log Z(t) = \sum_{r=1}^{\infty} N(q^r)t^r/r \quad \text{or} \quad tZ'(t)/Z(t) = \sum_{r=1}^{\infty} N(q^r)t^r,$$

then (3) is equivalent to

$$Z(t) = \frac{P_1(t,W)\cdots P_{2d-1}(t,W)}{P_0(t,W)P_2(t,W)\cdots P_{2d}(t,W)}$$

where $P_i(t,W) = \prod_j(1 - \alpha_{ij}t)$. Each $P_i(t,W)$ must have coefficients in $\mathbf{Z}$, and the analogue of the Riemann hypothesis is that $|\alpha_{ij}| = q^{i/2}$. (For a fuller account of Weil's conjectures and their motivation, see the excellent survey [19].) All this has now been proved, the main contributor being Deligne.

Now let $V$ be a nonsingular and absolutely irreducible projective variety defined over an algebraic number field $K$. If $V$ has good reduction at a prime $\mathfrak{p}$ of $K$ we can form $\tilde{V}_{\mathfrak{p}}$, the reduction of $V$ mod $\mathfrak{p}$, and hence form the $P_i(t, \tilde{V}_{\mathfrak{p}})$. For $s$ in $\mathbf{C}$, we can now define the *i*th global L-series $L_i(s, V)$ of $V$ as a product over all places of $K$, the factor at a prime $\mathfrak{p}$ of good reduction being $(P_i(q^{-s}, \tilde{V}_{\mathfrak{p}}))^{-1}$ where $q = \text{Norm}_{K/\mathbf{Q}}\mathfrak{p}$. The rules for forming the factors at the primes of bad reduction and at the infinite places can be found in [20]. These L-series of course depend on $K$ as well as on $V$. In particular, $L_0(s, V)$ is just the zeta-function of the algebraic number field $K$.

To call a function $F(s)$ a (global) zeta-function or L-series ought to carry with it certain implications, though some authors have used these terms very loosely:

- $F(s)$ should be the product of a Dirichlet series and possibly some Gamma-functions, and the half-plane of absolute convergence for the Dirichlet series should have the form $\Re s > \sigma_0$ with $2\sigma_0$ in $\mathbf{Z}$.
- The Dirichlet series should be expressible as an Euler product $\prod_p f_p(p^{-s})$ where the $f_p$ are rational functions.
- $F(s)$ should have an analytic continuation to the entire $s$-plane as a meromorphic function all of whose poles are in $\mathbf{Z}$.
- There should be a functional equation relating $F(s)$ and $F(2\sigma_0 - 1 - s)$.
- The zeroes of $F(s)$ in the critical strip $\sigma_0 - 1 < \Re s < \sigma_0$ should lie on $\Re s = \sigma_0 - \frac{1}{2}$.

In our case, the first two implications are trivial; and fortunately one is not expected to prove the last three, but only to state them as conjectures. The last one is the Riemann Hypothesis, which appears to be out of reach even in the simplest case, which is the classical Riemann zeta-function; and the third and fourth have so far only been proved in a few favourable cases.

*Question 3.1.* Can one extend the list of $V$ for which analytic continuation and the functional equation can be proved?

It seems likely that any proof of analytic continuation will carry a proof of the functional equation with it.

It has been said about the zeta-functions of algebraic number fields that "the zeta-function knows everything about the number field; we just have to prevail on it to

tell us". If this is so, we have not yet unlocked the treasure-house. Apart from the classical formula which relates $hR$ to $\zeta_K(0)$ all that has so far been proved are certain results of Borel [21] which relate the behaviour of $\zeta_K(s)$ near $s = 1 - m$ for integers $m > 1$ to the K-groups of $\mathfrak{O}_K$. One might hope that when a mysterious number turns up in the study of Diophantine problems on $V$, some L-series contains information about it; and this is certainly sometimes true, the most spectacular examples being the Birch/Swinnerton-Dyer conjecture and the far-reaching generalizations of it due to Bloch and Kato. But it appears to be false for the order of the Chow group of a rational surface; this is always finite, but two such surfaces can have the same L-series while having Chow groups of different orders.

Suppose for convenience that $V$ is defined over $\mathbf{Q}$, and let its dimension be $d$. Even for varieties with $B_1 = 0$ we do not expect a product like

$$\prod_p N(p)/p^d \quad \text{or} \quad \prod_p N(p) \Big/ \left( \frac{p^{d+1} - 1}{p - 1} \right) \tag{4}$$

to be necessarily absolutely convergent. But in some contexts there is a respectable expression which is formally equivalent to one of these, with appropriate modifications of the factors at the bad primes. The idea that such an expression should have number-theoretic significance goes back to Siegel (for genera of quadratic forms) and Hardy/Littlewood (for what they called the *singular series*). Using the ideas above, we are led to replace the study of the products (4) by a study of the behaviour of $L_{2d-1}(s,V)$ and $L_{2d-2}(s,V)$ near $s = d$. By duality, this is the same as studying $L_1(s,V)$ near $s = 1$ and $L_2(s,V)$ near $s = 2$. The information derived in this way appears to relate to the Picard group of $V$, defined as the group of divisors defined over $\mathbf{Q}$ modulo linear equivalence. By considering simultaneously both $V$ and its Picard variety (the abelian variety which parametrises divisors algebraically equivalent to zero modulo linear equivalence), one concludes that $L_1(s,V)$ should be associated with the Picard variety and $L_2(s,V)$ with the group of divisors modulo algebraic equivalence – that is, with the Néron-Severi group of $V$. These ideas motivated the weak forms of the Birch/Swinnerton-Dyer conjecture (for which see Sect. 4) and the case $m = 1$ of the Tate conjecture below. For the strong forms (which give expressions for the leading coefficients of the relevent Laurent series expansions) heuristic arguments are less convincing; but one can formulate conjectures for these coefficients by asking what other mysterious numbers turn up in the same context and should therefore appear in the formulae for the leading coefficients.

The weak form of the Tate conjecture asserts that the order of the pole of $L_{2m}(s,V)$ at $s = m + 1$ is equal to the rank of the group of classes of $m$-cycles on $V$ defined over $K$, modulo algebraic equivalence; it is a natural generalization of the case $m = 1$ for which the heuristics have just been shown. For a more detailed account of both of these, including the conjectural formulae for the leading coefficients, see [22] or [23].

*Question 3.2.* What information about $V$ is contained in its L-series?

There is in the literature a beautiful edifice of conjecture, lightly supported by evidence, about the behaviour of the $L_i(s,V)$ at integral points. The principal architects of this edifice are Beilinson, Bloch and Kato. Beilinson's conjectures relate to the order and leading coefficients of the Laurent series expansions of the $L_i(s,V)$ at integer values of $s$; in them the leading coefficients are treated as elements of $\mathbf{C}^*/\mathbf{Q}^*$. (For a full account see [24] or [25].) Bloch and Kato [26, 27] have strengthened these conjectures by treating the leading coefficients as elements of $\mathbf{C}^*$. But I do not believe that anything like the full story has yet been revealed.

# 4   Curves

The most important invariant of a curve is its genus $g$. In the language of algebraic geometry over $\mathbf{C}$, curves of genus 0 are called *rational*, curves of genus 1 are called *elliptic* and curves of genus greater than 1 are *of general type*. But note that for a number theorist an elliptic curve is defined to be a curve of genus 1 with a distinguished point $P_0$ on it, both being defined over the ground field $K$. The effect of this is that the points on an elliptic curve form an abelian group with $P_0$ as its identity element, the sum of $P_1$ and $P_2$ being the other zero of the function (defined up to multiplication by a constant) with poles at $P_1$ and $P_2$ and a zero at $P_0$.

A canonical divisor on a curve $\Gamma$ of genus 0 has degree $-2$; hence by the Riemann-Roch theorem $\Gamma$ is birationally equivalent over the ground field to a conic. The Hasse principle holds for conics, and therefore for all curves of genus 0; this gives a complete answer to Question (A) at the beginning of these notes. But it does not give an answer to Question (B). Over $\mathbf{Q}$, a very simple answer to Question (B) is as follows:

**Theorem 4.1.** *Let* $a_0, a_1, a_2$ *be nonzero elements of* $\mathbf{Z}$*. If the equation*

$$a_0 X_0^2 + a_1 X_1^2 + a_2 X_2^2 = 0$$

*has a nontrivial solution in* $\mathbf{Z}$*, then it has a solution for which each* $a_i X_i^2$ *is absolutely bounded by* $|a_0 a_1 a_2|$*.*

Siegel [28] has given an answer to Question (B) over arbitrary algebraic number fields, and Raghavan [29] has generalized Siegel's work to quadratic forms in more variables.

The knowledge of one rational point on $\Gamma$ enables us to transform $\Gamma$ birationally into a line; so if $\Gamma$ is soluble there is a parametric solution which gives explicitly all the points on $\Gamma$ defined over the ground field. This answers Question (C).

If $\Gamma$ is a curve of general type defined over an algebraic number field $K$, Mordell conjectured and Faltings proved that $\Gamma(K)$ is finite; and a number of other proofs have appeared since then. But it does not seem that any of them enable one to compute $\Gamma(K)$, though some of them come tantalizingly close. For a survey of several such proofs, see [30].

*Question 4.2.* Is there an algorithm for computing $\Gamma(\mathbf{Q})$ when $\Gamma$ is a curve of general type defined over $\mathbf{Q}$?

The study of rational points on elliptic curves is now a major industry, almost entirely separate from the study of other Diophantine problems. If $\Gamma$ is an elliptic curve defined over an algebraic number field $K$, the group $\Gamma(K)$ is called the *Mordell-Weil group*. Mordell proved that $\Gamma(K)$ is finitely generated and Weil extended this to all Abelian varieties. Thanks to Mazur [31] and Merel [32] the theory of the torsion part of the Mordell-Weil group is now reasonably complete; but for the non-torsion part all that was known before 1960 is that for any $n > 1$ $\Gamma(K)/n\Gamma(K)$ could be embedded into a certain group (the $n$-Selmer group, for which see Sect. 10) which is finitely generated and computable. The process involved, which is known as the method of infinite descent, goes back to Fermat; various forms of this for $n = 2$ will be described in Sect. 10. By means of this process one can always compute an upper bound for the rank of the Mordell-Weil group of any particular $\Gamma$, and the upper bound thus obtained can frequently be shown to be equal to the actual rank by exhibiting enough elements of $\Gamma(K)$. It was also conjectured that the difference between the upper bound thus computed and the actual rank was always an even integer, but apart from this the actual rank was mysterious. This not wholly satisfactory state of affairs has been radically changed by the Birch/Swinnerton-Dyer conjecture, the weak form of which is described at the end of this section. A survey of what is currently known or conjectured about the ranks of Mordell-Weil groups can be found in [33].

Suppose now that $\Gamma$ is a curve of genus 1 defined over $K$ but not necessarily containing a point defined over $K$. Let $J$ be the Jacobian of $\Gamma$, defined as a curve whose points are in one-one correspondence with the divisors of degree 0 on $\Gamma$ modulo linear equivalence. Then $J$ is also a curve of genus 1 defined over $K$, and $J(K)$ contains the point which corresponds to the trivial divisor. So $J$ is an elliptic curve in our sense.

Conversely, if we fix an elliptic curve $J$ defined over $K$ we can consider the equivalence classes (for birational equivalence over $K$) of curves $\Gamma$ of genus 1 defined over $K$ which have $J$ as Jacobian. For number theory, the only ones of interest are those which contain points defined over each completion $K_v$. These form a commutative torsion group, called the *Tate-Shafarevich group* and usually denoted by Ш; the identity element of this group is the class which contains $J$ itself, and it consists of those $\Gamma$ which have $J$ as Jacobian and which contain a point defined over $K$. (The simplest example of a nontrivial element of a Tate-Shafarevich group is the curve

$$3X_0^3 + 4X_1^3 + 5X_2^3 = 0 \quad \text{with Jacobian} \quad Y_0^3 + Y_1^3 + 60Y_2^3 = 0.)$$

Thus for curves of genus 1 the Tate-Shafarevich group is by definition the obstruction to the Hasse principle.

The weak form of the Birch/Swinnerton-Dyer conjecture states that the rank of the Mordell-Weil group of an elliptic curve $J$ is equal to the order of the zero of $L_1(s, J)$ at $s = 1$; the conjecture also gives an explicit formula for the leading coefficient of the power series expansion at that point. Note that this point is at the

centre of the critical strip, so that the conjecture pre-supposes the analytic continuation of $L_1(s,J)$. At present there are two well-understood cases in which analytic continuation is known: when $K = \mathbf{Q}$, so that $J$ can be parametrised by means of modular functions, and when $J$ admits complex multiplication. In consequence, these two cases are likely to be easier than the general case; but even here I do not expect much further progress in the next decade. In each of these two cases, if one assumes the Birch/Swinnerton-Dyer conjecture one can derive an algorithm for finding the Mordell-Weil group and the order of the Tate-Shafarevich group; and in the first of the two cases this algorithm has been implemented by Gebel [34]. Without using the Birch/Swinnerton-Dyer conjecture, Heegner long ago produced a way of generating a point on $J$ whenever $K = \mathbf{Q}$ and $J$ is modular; and Gross and Zagier [35, 36] have shown that this point has infinite order precisely when $L'(1,J) \neq 0$. Building on their work, Kolyvagin (see [37]) has shown the following.

**Theorem 4.3.** *Suppose that the Heegner point has infinite order; then the group $J(\mathbf{Q})$ has rank 1 and $\text{Ш}(J)$ is finite.*

Kolyvagin [38] has also obtained sufficient conditions for both $J(\mathbf{Q})$ and $\text{Ш}(J)$ to be finite. The following result is due to Nekovar and Plater.

**Theorem 4.4.** *If the order of $L(s,J)$ at $s = 1$ is odd then either $J(\mathbf{Q})$ is infinite or the p-part of $\text{Ш}(J)$ is infinite for every good ordinary p.*

If $J$ is defined over an algebraic number field $K$ and can be parametrized by modular functions for some arithmetic subgroup of $\text{SL}_2(\mathbf{R})$ then analytic continuation and the functional equation for $L_1(s,J)$ follow; but there is not even a plausible conjecture identifying the $J$ which have this property, and there is no known analogue of Heegner's construction.

In the complex multiplication case, what is known is as follows.

**Theorem 4.5.** *Let K be an imaginary quadratic field and J an elliptic curve defined and admitting complex multiplication over K. If $L(1,J) \neq 0$, then*

 (i) *$J(K)$ is finite;*
(ii) *For every prime $p > 7$ the p-part of $\text{Ш}(J)$ is finite and has the order predicted by the Birch/Swinnerton-Dyer conjecture.*

Here (i) is due to Coates and Wiles, and (ii) to Rubin. For an account of the proofs, see [39]. Katz has generalized (i) and part of (ii) to behaviour over an abelian extension of $\mathbf{Q}$, but with the same $J$ as before.

In general we do not know how to compute $\text{Ш}$. It is conjectured that it is always finite; and indeed this assertion can be regarded as part of the Birch/Swinnerton-Dyer conjecture, for the formula for the leading coefficient of the power series for $L_1(s,J)$ at $s = 1$ contains the order of $\text{Ш}(J)$ as a factor. If indeed this order is finite, then it must be a square; for Cassels has proved the existence of a skew-symmetric bilinear form on $\text{Ш}$ with values in $\mathbf{Q}/\mathbf{Z}$, which is nonsingular on the quotient of $\text{Ш}$ by its maximal divisible subgroup. In particular, finiteness implies that if $\text{Ш}$ contains at most $p - 1$ elements of order exactly $p$ for some prime $p$ then it actually

contains no such elements; hence an element which is killed by $p$ is trivial, and the curves of genus 1 in that equivalence class contain points defined over $K$. For use later, we state the case $p = 2$ as a lemma.

**Lemma 4.6.** *Suppose that* $\text{III}(J)$ *is finite and the quotient of the* 2-*Selmer group of* $J$ *by its soluble elements has order at most* 2; *then that quotient is actually trivial.*

# 5  Varieties of Higher Dimension and the Hardy-Littlewood Method

A first coarse classification of varieties of dimension $n$ is given by the *Kodaira dimension* $\kappa$, which can take the values $-\infty$ or $0, 1, \ldots, n$. Denote the genus of a curve by $g$; then for curves $\kappa = -\infty$ corresponds to $g = 0$, $\kappa = 0$ to $g = 1$ and $\kappa = 1$ to $g > 1$; so the major split in the Diophantine theory of curves corresponds to the possible values of $\kappa$.

Over $\mathbf{C}$ a full classification of surfaces can be found in [40]. But what is also significant for the number theory (and cuts across this classification) is whether the surface is *elliptic* – that is, whether over $\mathbf{C}$ there is a map $V \to C$ for some curve $C$ whose general fibre is a curve of genus 1. The case when the map $V \to C$ is defined over the ground field $K$ and $C$ has genus 0 is discussed below; in this case the Diophantine problems for $V$ are only of interest when $C(K)$ is nonzero, so that $C$ can be identified with $\mathbf{P}^1$. When $C$ has genus greater than 1, the map $V \to C$ is essentially unique and it and $C$ are therefore both defined over $K$. By Faltings' theorem, $C(K)$ is then finite; thus each point of $V(K)$ lies on one of a finite set of fibres, and it is enough to study these. In contrast, we know nothing except in very special cases when $C$ is elliptic.

The surfaces with $\kappa = -\infty$ are precisely the *ruled surfaces* – that is, those which are birationally equivalent over $\mathbf{C}$ to $\mathbf{P}^1 \times C$ for some curve $C$. Among these, by far the most interesting are the *rational surfaces*, which are birationally equivalent to $\mathbf{P}^2$ over $\mathbf{C}$. From the number-theoretic point of view, there are two kinds of rational surface:

- Pencils of conics, given by an equation of the form

$$a_0(u,v)X_0^2 + a_1(u,v)X_1^2 + a_2(u,v)X_2^2 = 0 \tag{5}$$

  where the $a_i(u,v)$ are homogeneous polynomials of the same degree. Pencils of conics can be classified in more detail according to the number of bad fibres.
- Del Pezzo surfaces of degree $d$, where $0 < d \leq 9$. Over $\mathbf{C}$, such a surface is obtained by blowing up $(9 - d)$ points of $\mathbf{P}^2$ in general position – except when $d = 8$, in which case the construction is more complicated. It is known that Del Pezzo surfaces of degree $d > 4$ satisfy the Hasse principle and weak approximation; indeed those of degree 5 or 7 necessarily contain rational points. Del Pezzo surfaces of degree 2 or 1 have attracted relatively little attention; it seems sen-

sible to ignore them until the problems coming from those of degrees 4 and 3 have been solved. The Del Pezzo surfaces of degree 3 are the nonsingular cubic surfaces, which have an enormous but largely irrelevant literature, and those of degree 4 are the nonsingular intersections of two quadrics in $\mathbf{P}^4$. For historical reasons, attention has been concentrated on the Del Pezzo surfaces of degree 3; but the problems presented by those of degree 4 are necessarily simpler.

Surfaces with $\kappa = 0$ fall into four families:

- Abelian surfaces. These are the analogues in two dimensions of elliptic curves, and there is no reason to doubt that their number-theoretical properties largely generalize those of elliptic curves.
- K3 surfaces, including in particular Kummer surfaces. Some but not all K3 surfaces are elliptic.
- Enriques surfaces, whose number theory has been very little studied. Enriques surfaces are necessarily elliptic.
- Bielliptic surfaces.

Surfaces with $\kappa = 1$ are necessarily elliptic.

Surfaces with $\kappa = 2$ are called *surfaces of general type* – which in mathematics is generally a derogatory phrase. About them there is currently nothing to say beyond Lang's conjecture stated in Sect. 2.

For varieties of higher dimension (other than quadrics and Severi-Brauer varieties) there seem to be at the moment only two ways of obtaining results: by deduction from special results for surfaces, and by the Hardy/Littlewood method. The latter differs from most geometric methods in that it is not concerned with an equivalence class of varieties under birational or biregular transformation, but with a particular embedding of a variety $V$ in projective or affine space. A point $P$ in $\mathbf{P}^n$ defined over $\mathbf{Q}$ has a representation $(x_0, \ldots, x_n)$ where the $x_i$ are integers with no common factor; and this representation is unique up to changing the signs of all the $x_i$. We define the *height* of $P$ to be $h(P) = \max |x_i|$; a linear transformation on the ambient space multiplies heights by numbers which lie between two positive constants depending on the linear transformation. Denote by $N(H,V)$ the number of points of $V(\mathbf{Q})$ whose height is less than $H$; then it is natural to ask how $N(H,V)$ behaves as $H \to \infty$. This is the core question for the Hardy-Littlewood method, which when it is applicable is the best (and often the only) way of proving that $V(\mathbf{Q})$ is not empty. In very general circumstances that method provides estimates of the form

$$N(H,V) = \text{ leading term } + \text{ error term.} \tag{6}$$

The leading term is usually the same as one would obtain by probabilistic arguments. But such results are only valuable when it can be shown that the error term is small compared to the leading term, and to achieve this the dimension of $V$ needs to be large compared to its degree. The extreme case of this is the following theorem, due to Birch [41].

**Theorem 5.1.** *Suppose that the $F_i(X_0, \ldots, X_N)$ are homogeneous polynomials with coefficients in $\mathbf{Z}$ and $\deg F_i = r_i$ for $i = 1, \ldots, m$, where $r_1, \ldots, r_m$ are positive odd*

*integers. Then there exists $N_0(r_1,\ldots,r_m)$ such that if $N \geq N_0$ the $F_i$ have a common nontrivial zero in $\mathbf{Z}^{N+1}$.*

The proof falls into two parts. First, the Hardy-Littlewood method is used to prove the result in the special case when $m = 1$ and $F_1$ is diagonal – that is, to show that if $r$ is odd and $N \geq N_1(r)$ then

$$c_0 X_0^r + \ldots + c_N X_N^r = 0$$

has a nontrivial integral solution. Then the general case is reduced to this special case by purely elementary methods. The requirement that all the $r_i$ should be odd arises from difficulties connected with the real place; over a fixed totally complex algebraic number field there is a similar theorem for which the $r_i$ can be any positive integers.

The Hardy-Littlewood method was designed for a single equation in which the variables are separated – for example, an equation of the form

$$f_1(X_1) + \ldots + f_N(X_N) = c$$

where the $f_i$ are polynomials, the $X_i$ are integers, and one wishes to prove solubility in $\mathbf{Z}$ for all integers $c$, or all large enough $c$, or almost all $c$. But it has also been applied both to several simultaneous equations and to equations in which the variables are not separated. The following theorem of Hooley [42] is the most impressive result in this direction.

**Theorem 5.2.** *Homogeneous nonsingular nonary cubics over $\mathbf{Q}$ satisfy both the Hasse principle and weak approximation.*

# 6 Manin's Conjecture

Even on the most optimistic view, one can only hope to make the Hardy-Littlewood method work for families for which $N(H,V)$ is asymptotically equal to its probabilistic value; in particular it seems unlikely that it can be made to work for families for which weak approximation fails. On the other hand, one can hope that the leading term in (6) will still have the correct shape for other families, even if it is in error by a constant factor. Manin has put forward a conjecture about the asymptotic density of rational solutions for certain geometrically interesting families of varieties for which weak approximation is unlikely to hold: more precisely, for Fano varieties embedded in $\mathbf{P}^n$ by means of their anticanonical divisors. A general survey of the present state of the Manin conjecture can be found in [43]. In the full generality in which he stated the conjecture, it is known to be false; and in what follows I consider it only for Del Pezzo surfaces $V$ of degrees 3 and 4. These are the most natural ones for the number theorist to consider, because of the simplicity of the equations which define them – one cubic and two quadratic respectively. The anal-

ogy of the Hardy-Littlewood method suggests an estimate $AH\prod(N(p)/(p+1))$ for $N(H,V)$, where the product is taken over all primes less than a certain bound which depends on $H$. In view of what is said in Sect. 3, this product ought to be replaced by something which depends on the behaviour of $L_2(s,V)$ near $s = 1$. The way in which the leading term in the Hardy-Littlewood method is obtained suggests that here we should take $s - 1$ to be comparable with $(\log H)^{-1}$. Remembering the Tate conjecture, this gives the right hand side of (7) as a conjectural estimate for $N(H,V)$. But to ask about $N(H,V)$ is the wrong question, for $V$ may contain lines $L$ defined over $\mathbf{Q}$, and for any line $N(H,L) \sim AH^2$ for some nonzero constant $A$. This is much greater than the order-of-magnitude estimate for $N(H,V)$ given by a probabilistic argument. Manin's way to resolve this absurdity is to study not $N(H,V)$ but $N(H,U)$, where $U$ is the open subset of $V$ obtained by deleting the finitely many lines on $V$. He therefore conjectured that

$$N(H,U) \sim AH(\log H)^{r-1} \text{ where } r \text{ is the rank of } \mathrm{Pic}(V). \tag{7}$$

Peyre [44] has given a conjectural formula for $A$. Unfortunately there are no nonsingular Del Pezzo surfaces of degrees 3 or 4, and very few singular ones, for which (7) has been proved.

*Question 6.1.* Are there nonsingular Del Pezzo surfaces $V$ of degree 3 or 4 for which the Manin conjecture can be proved by present methods?

In the first instance, it would be wise to address this problem under rather restrictive hypotheses about $V$, not least because the Brauer-Manin obstruction to weak approximation occurs in the conjectural formula for $A$ and therefore the problem is likely to be easier for families of $V$ for which weak approximation holds. The simplest cases of all are likely to be among those for which $V$ is birationally equivalent to $\mathbf{P}^2$ over $\mathbf{Q}$. For nonsingular cubic surfaces, for example, it has long been known that this happens if and only if $V$ is everywhere locally soluble and contains a divisor defined over $\mathbf{Q}$ which is the union of 2, 3 or 6 skew lines. In the case when $V$ contains two skew lines each defined over $\mathbf{Q}$, a lower bound for $N(H,U)$ of the correct order of magnitude was proved in [45].

An alternative method of describing the statistics of rational points on $U$ is by means of the *height zeta function*

$$Z(h,U,s) = \sum_{P \in U(\mathbf{Q})}(h(P))^{-s}$$

where $h$ is some height function – for example, the classical one defined in Sect. 5. (Note that, despite the name, we do not expect this function to have the properties listed in Sect. 3.) Now (7) is more or less equivalent to

$$Z(h,U,s) \sim A'(s-1)^{-r} \text{ as } s \text{ tends to 1 from above.}$$

It is now natural to hope that $Z(h,U,z)$ can be analytically continued to some halfplane $\Re s > c$ for some $c < 1$, subject to a pole of order $r$ at $s = 1$. If this is

so, we can derive $N(H,U)$ from $Z(U,s)$ by means of Perron's formula

$$N(H,U) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} B^s \frac{Z(U,s)}{s} ds$$

where $H-1 < B < H$ and $c > 1$. Now (7) can be strengthened to

$$N(H,U) = H f(\log H) + O(H^{c+\varepsilon}) \tag{8}$$

where $f$ is a polynomial of degree $r-1$.

De la Bretèche and Browning [46, 47, 48] have proved results of the form (8) for several singular Del Pezzo surfaces of degrees 3 and 4. Their methods are intricate, and it would be interesting to know what features of the geometry of their particular surfaces underlie them. The simplest surface of this kind, and the one about which most is known, is the toric surface

$$X_0^3 = X_1 X_2 X_3. \tag{9}$$

Let $U$ be the open subset of (9) given by $X_0 \neq 0$. Building on earlier work of de la Bretèche [49] and assuming the Riemann Hypothesis, he and I have proved [50] that

$$N(U,H) = H f(\log H) + C H^{9/11} + \Re \sum \gamma_n H^{3/4+\rho_n/8} + O(H^{4/5}) \tag{10}$$

where $C$ and the $\gamma_n$ are constants, $\rho_n$ runs through the zeros of the Riemann zeta function, and $f$ is a certain polynomial of degree 6. Some bracketing of terms for which the $\rho_n$ are nearly equal may be needed to ensure convergence. The associated height zeta function can be meromorphically continued to $\Re s > \frac{3}{4}$ but no further.

The key idea in the proofs of (10) and of analytic continuation is to introduce the multiple Dirichlet series

$$\phi(s_1,s_2,s_3) = \sum_{P \in U(\mathbf{Q})} |x_1|^{-s_1} |x_2|^{-s_2} |x_3|^{-s_3}$$

where $(x_0,x_1,x_2,x_3)$ is a primitive integral representation of $P$. At the cost of a factor 4, we can confine ourselves in the definition of $\phi$ to points with all coordinates positive. We have

$$|x_1|^{-s_1} |x_2|^{-s_2} |x_3|^{-s_3} = \prod_p p^{-\{s_1 v_p(x_1) + s_2 v_p(x_2) + s_3 v_p(x_3)\}}$$

from which it follows that $\phi(s_1,s_2,s_3) = 4 \prod_p \phi^*(p^{-s_1}, p^{-s_2}, p^{-s_3})$ where the factor associated with $p$ is the sum over the points all of whose coordinates are powers of $p$. A straightforward calculation shows that

$$\phi^*(z_1,z_2,z_3) = \frac{1 + \sum z_i^2 z_j (1 - z_k^3) - z_1^3 z_2^3 z_3^3}{(1 - z_1^3)(1 - z_2^3)(1 - z_3^3)},$$

the sum being taken over the six permutations $i, j, k$ of 1, 2, 3. This expresses $\phi(s_1, s_2, s_3)$ as an Euler product and enables its meromorphic continuation to the open set in which $\Re s_i > 0$ for $i = 1, 2, 3$. (A simpler example of the same process will be found in the next paragraph.) Moreover

$$Z(h, U, s) = \frac{1}{(2\pi i)^2} \int_{c_2 - i\infty}^{c_2 + i\infty} \int_{c_3 - i\infty}^{c_3 + i\infty} \frac{s\phi(s - s_2 - s_3, s_2, s_3)}{s_2 s_3 (s - s_2 - s_3)} ds_2 ds_3$$

provided $\Re s, c_2$ and $c_3$ are chosen so that the series for $\phi$ is absolutely convergent. One can now move the contours of integration to the left, though the reader is warned that this imvolves technical problems as well as some tedious calculation. In the end (10) and the meromorphic continuation of $Z(h, U, s)$ follow.

The estimate (10) is reminiscent of the explicit formula of prime number theory. But the second term on the right is unexpected, and one would have hoped that the exponent in the third term would have been $\rho_n$ rather than $\frac{3}{4} + \frac{1}{8}\rho_n$. Both these blemishes are caused by the fact that $h(P)$, though classical, is not the most natural height function. For comparison, we now consider what happens if we use as our height function $h_1(P) = |x_0|$ where $(x_0, x_1, x_2, x_3)$ is a primitive integral representation of $P$. Now we obtain

$$Z(h_1, U, s) = 4 \prod_p \frac{1 + 7p^{-s} + p^{-2s}}{(1 - p^{-s})^2}.$$

The factor corresponding to $p$ on the right is

$$(1 - p^{-s})^{-9} \{(1 - p^{-s})^7 (1 + 7p^{-s} + p^{-2s})\}$$

where the expression in curly brackets is $1 + O(p^{-2s})$; so using the known analytic continuation of the Riemann zeta function, this gives the continuation of $Z(h_1, U, s)$ to $\Re s > \frac{1}{2}$. The expression in curly brackets is actually

$$1 - 27p^{-2s} + O(p^{-3s});$$

so we can take out a factor $(1 - p^{-2s})^{27}$ and obtain the continuation of $Z(h_1, U, s)$ to $\Re s > \frac{1}{3}$ – and so on. The eventual conclusion is that $Z(h_1, U, s)$ can be meromorphically continued to $\Re s > 0$ but that $\Re s = 0$ is a natural boundary. Using Perron's formula we can obtain a complicated formula for the corresponding counting function $N_1(H, U)$ of which the leading terms are

$$N_1(H, U) = H f_1(\log H) + H^{1/3} g_1(\log H) + \sum \gamma_{1n}(\log H) H^{\rho_n/2} + O(H^{1/5 + \varepsilon}).$$

Here $f_1$ and $g_1$ are polynomials of degrees 8 and 104 respectively, $\rho_n$ runs through the complex zeros of the Riemann zeta function and the $\gamma_{1n}$ are polynomials of degree 26.

The second term here is much smaller than that in (10). This raises the question of what is the best height function to choose, and indeed whether there is a canonical height function on at least some Del Pezzo surfaces. (Recall that on abelian varieties

there certainly is a canonical height function.) A very partial answer to this can be found in [51], where reasons are given for using for (9) the height function $h^*(P) = \prod_p p^{-s\alpha_p}$ where

$$\alpha_p = \frac{1}{2}((v_p(x_1))^2 + (v_p(x_2))^2 + (v_p(x_3))^2 - 3(v_p(x_0))^2).$$

With this choice, again assuming the Riemann Hypothesis, the natural boundary for the height zeta function $Z(h^*, U, s)$ is $\Re s = 0$ and we can exhibit a (very complicated) formula for the corresponding counting function $N^*(H, U)$ with error $O(H^\varepsilon)$. This time the polynomial $f^*$ in the leading term $Hf^*(\log H)$ has degree 5 and the remaining terms contribute $O(H^{1/2+\varepsilon})$.

In the light of these results it is natural to wonder what is the shape of the error term in (8) when $V$ is nonsingular. At present, the only way to approach this question is by computation. It is advantageous to study varieties whose equations have the form $g_1(X_0, X_1) = g_2(X_2, X_3)$ because counting rational points is then much faster than for general cubic surfaces. Some computations have been made for $V$ of the form

$$a_0X_0^3 + a_1X_1^3 + a_2X_2^3 + a_3X_3^3 = 0.$$

Now $r = 1$ and the evidence strongly suggests that in (8) we can take $c = \frac{1}{2}$. The results are indeed compatible with a conjecture of the form

$$N(H, V) = AH + \sum \gamma_n H^{1/2+it_n} + O(H^{1/2-\varepsilon}) \tag{11}$$

for a discrete sequence of real $t_n$. But the evidence available so far, which is for $H \leq 10^5$, is too scanty for one to be able to estimate the first few $t_n$ with any great accuracy. However, the way in which they appear in (11) suggests that they should be the zeros of some L-series – and of course there is one L-series naturally associated with $V$.

There is no reason why one should not also ask about the density of rational points on surfaces which are not Fano. For Del Pezzo surfaces, the conjectural value of $c$ for which $N(H, U) \sim AH(\log H)^c$ is defined by the geometry rather than by the number theory, though that is not true of $A$. For other varieties, the corresponding statement need no longer be true. We start with curves. For a curve of genus 0 and degree $d$, we have $N(H, V) \sim AH^{2/d}$; and for a curve of genus greater than 1 Faltings' theorem is equivalent to the statement that $N(H, V) = O(1)$. But if $V$ is an elliptic curve then $N(H, V) \sim A(\log H)^{r/2}$ where $r$ is the rank of the Mordell-Weil group. (For elliptic curves there is a more canonical definition of height, which is invariant under bilinear transformation; this is used to prove the result above.)

For pencils of conics, Manin's question is probably not the best one to ask, and it would be better to proceed as follows. A pencil of conics is a surface $V$ together with a map $V \to \mathbf{P}^1$ whose fibres are conics. Let $N^*(H, V)$ be the number of points on $\mathbf{P}^1$ of height less than $H$ for which the corresponding fibre contains rational points.

*Question 6.2.* What is the conjectural estimate for $N^*(H,V)$ and under what conditions can one prove it?

It may be worth asking the same questions for pencils of curves of genus 1.

For surfaces of general type, Lang's conjecture implies that questions about $N(H,V)$ are really questions about certain curves on $V$; and for Abelian surfaces (and indeed Abelian varieties in any dimension) the obvious generalisation of the theorem for elliptic curves holds. The new case of greatest interest is that of K3 surfaces, and in particular that of nonsingular quartic surfaces. The same heuristics which led to (7) for Del Pezzo surfaces now lead one to

$$N(H,V) \sim A(\log H)^r \tag{12}$$

where $r$ is as before the rank of $\mathrm{Pic}(V)$. Unfortunately, if $V$ contains at least one soluble curve of genus 0 it contains infinitely many; and on each one of them the rational points will outnumber the estimate given by (12). To delete all these curves and count the rational points on what is left appears neither sensible nor feasible; so we have to assume that $V$ contains no such curves. If $V$ contains a pencil of curves of genus 1 it again seems unlikely that (12) can hold. Van Luijk has tabulated $N(H,V)$ for certain quartic surfaces which have neither of these properties and which have $r = 1$ or 2, and his results fit the conjecture (12) very well.

# 7   Schinzel's Hypothesis and Salberger's Device

Schinzel's Hypothesis gives a conjectural answer to the following question: given finitely many polynomials $F_1(X),\ldots,F_n(X)$ in $\mathbf{Z}[X]$ with positive leading coefficients, is there an arbitrarily large integer $x$ at which they all take prime values? There are two obvious obstructions to this:

- One or more of the $F_i(X)$ may factorize in $\mathbf{Z}[X]$.
- There may be a prime $p$ such that for any value of $x \bmod p$ at least one of the $F_i(x)$ is divisible by $p$.

If the congruence $F_i(x) \equiv 0 \bmod p$ is non-trivial, it has at most $\deg(F_i)$ solutions; so the second obstruction can only happen for $p \leq \sum \deg(F_i)$ or if $p$ divides every coefficient of some $F_i$. Schinzel's Hypothesis is that these are the only obstructions: in other words, if neither of them happens then we can choose an arbitrarily large $x$ so that every $F_i(x)$ is a prime.

If one assumes Schinzel's Hypothesis the corresponding result over any algebraic number field follows easily. But in most applications there is a predetermined set $\mathfrak{B}$ of bad places, and we need to impose local conditions on $x$ at some or all of them. These conditions constrain the values of the $F_i(x)$ at those places, and therefore we cannot necessarily require these values to be units at the bad primes; nor in the applications do we need to. I have stated Lemma 7.1 in a form which applies to homogeneous polynomials $G_i$ in two variables; but the reader who wishes to

do so will have no difficulty in stating and proving the corresponding (stronger) result for polynomials in one variable. Just as with the original version of Schinzel's Hypothesis, provided that the coefficients of $G_i$ for each $i$ have no common factor we need only verify the existence of the $y_\mathfrak{p}, z_\mathfrak{p}$ in the statement of the lemma when the absolute norm of $\mathfrak{p}$ does not exceed $\sum \deg(G_i)$.

**Lemma 7.1.** *Let $k$ be an algebraic number field and $\mathfrak{o}$ the ring of integers of $k$. Let $G_1(Y,Z),\ldots,G_n(Y,Z)$ be homogeneous irreducible elements of $\mathfrak{o}[Y,Z]$ and $\mathfrak{B}$ a finite set of primes of $k$. Suppose that for each $\mathfrak{p}$ not in $\mathfrak{B}$ there exist $y_\mathfrak{p}, z_\mathfrak{p}$ in $\mathfrak{o}$ such that none of the $G_i(y_\mathfrak{p}, z_\mathfrak{p})$ is in $\mathfrak{p}$. For each $\mathfrak{p}$ in $\mathfrak{B}$, let $V_\mathfrak{p}$ be a non-empty open subset of $k_\mathfrak{p} \times k_\mathfrak{p}$; and for each infinite place $v$ of $k$ let $V_v$ be a non-empty open subset of $k_v^*$. Assume Schinzel's Hypothesis; then there is a point $\eta \times \zeta$ in $k^* \times k^*$, with $\eta, \zeta$ integral outside $\mathfrak{B}$, such that*

- *$\eta \times \zeta$ lies in $V_\mathfrak{p}$ for each $\mathfrak{p}$ in $\mathfrak{B}$;*
- *$\eta/\zeta$ lies in $V_v$ for each infinite place $v$;*
- *Each ideal $(G_i(\eta,\zeta))$ is the product of a prime ideal not in $\mathfrak{B}$ and possibly powers of primes in $\mathfrak{B}$.*

*Proof.* Choose $\alpha, \beta$ in $\mathfrak{o}$ so that $\alpha/\beta$ lies in $V_v$ for each infinite place $v$ and no $G_i(\alpha,\beta)$ vanishes. We can repeatedly adjoin a further prime $\mathfrak{p}$ to $\mathfrak{B}$ provided we define the corresponding $V_\mathfrak{p}$ to be the set of all $y \times z$ in $\mathfrak{o}_\mathfrak{p} \times \mathfrak{o}_\mathfrak{p}$ such that each $G_i(y,z)$ is a unit at $\mathfrak{p}$. We can therefore assume that $\mathfrak{B}$ contains all ramified primes $\mathfrak{p}$ and all primes $\mathfrak{p}$ such that

- The absolute norm of $\mathfrak{p}$ is not greater than $[k:\mathbf{Q}]\sum \deg(G_i)$; or
- $\mathfrak{p}$ divides any $G_i(\alpha,\beta)$.

Let $\mathscr{B}$ be the set of primes in $\mathbf{Q}$ which lie below some prime of $\mathfrak{B}$, and further adjoin to $\mathfrak{B}$ all the primes of $k$ not already in $\mathfrak{B}$ which lie above some prime of $\mathscr{B}$. By the Chinese Remainder Theorem we can choose $\eta_0, \zeta_0$ in $k$, integral outside $\mathfrak{B}$ and such that each $G_i(\eta_0,\zeta_0)$ is nonzero and $\eta_0 \times \zeta_0$ lies in $V_\mathfrak{p}$ for each $\mathfrak{p}$ in $\mathfrak{B}$. For reasons which will become clear after (13), we also need to ensure that $\beta \eta_0 \neq \alpha \zeta_0$; this can be done by varying $\eta_0$ or $\zeta_0$ by a suitable element of $\mathfrak{o}$ divisible by large powers of each $\mathfrak{p}$ in $\mathfrak{B}$. As an ideal, write

$$(G_i(\eta_0,\zeta_0)) = \mathfrak{a}_i \mathfrak{b}_i$$

where the prime factors of each $\mathfrak{a}_i$ are outside $\mathfrak{B}$ and those of each $\mathfrak{b}_i$ are in $\mathfrak{B}$; thus $\mathfrak{a}_i$ is integral. Let $N_i$ be the absolute norm of $\mathfrak{b}_i$. Now choose $\gamma \neq 0$ in $\mathfrak{o}$ to be a unit at all the primes outside $\mathfrak{B}$ which divide any $G_i(\eta_0,\zeta_0)$ and to be divisible by such large powers of each $\mathfrak{p}$ in $\mathfrak{B}$ that

$$\eta \times \zeta = (\alpha\gamma\xi + \eta_0) \times (\beta\gamma\xi + \zeta_0)$$

is in $V_\mathfrak{p}$ for all $\xi \in \mathfrak{o}$ and all $\mathfrak{p} \in \mathfrak{B}$, and that if we write

$$g_i(X) = G_i(\alpha\gamma X + \eta_0, \beta\gamma X + \zeta_0), \tag{13}$$

then every coefficient of $g_i(X)$ is divisible by at least as great a power of $\mathfrak{p}$ as is $\mathfrak{b}_i$. We have arranged that the two arguments of $G_i$ in (13), considered as linear forms in $X$, are not proportional; thus if $g_i(X)$ factorizes in $k[X]$ then $G_i(\alpha\gamma U + \eta_0 V, \beta\gamma U + \zeta_0 V)$ would factorize in $k[U,V]$, contrary to the irreducibility of $G_i(Y,Z)$. We shall also require for each $i$ that $g_i(X)$ is prime to all its conjugates as elements of $\bar{k}[X]$; since the zeros of $g_i(X)$ have the form $\gamma^{-1}\xi_{ij}$ for some $\xi_{ij}$ independent of $\gamma$, this merely requires the ratios of $\gamma$ to its conjugates to avoid finitely many values. Write

$$R_i(X) = \mathrm{Norm}_{k(X)/\mathbf{Q}(X)}(g_i(X))/N_i;$$

then $R_i(X)$ has all its coefficients integral, for at each prime it is the norm of a polynomial with locally integral coefficients. An irreducible factor of $R_i(X)$ in $\mathbf{Q}[X]$ cannot be prime to $g_i(X)$, because then it would also be prime to all the conjugates of $g_i(X)$ and therefore to their product – which is absurd. If $R_i(X)$ had two coprime factors in $\mathbf{Q}[X]$, their highest common factors with $g_i(X)$ would be non-trivial coprime factors of $g_i(X)$ in $k[X]$, whence $g_i(X)$ would not be irreducible in $k[X]$. Finally, $R_i(X)$ cannot have a repeated factor because the conjugates of $g_i(X)$ are pairwise coprime. So $R_i(X) = A_i H_i(X)$ in $\mathbf{Z}[X]$, with $H_i(X)$ irreducible. Clearly we can require the leading coefficient of each $H_i(X)$ to be positive. But the only primes which divide the constant term in $R_i(X)$ are the primes outside $\mathscr{B}$ which divide $G_i(\eta_0, \zeta_0)$, and none of them divide the leading coefficient of $R_i(X)$; hence $A_i = \pm 1$. Now apply Schinzel's Hypothesis to the $H_i(X)$, which we can do because no $H_i(0)$ is divisible by any prime in $\mathscr{B}$. But if $H_i(x)$ is equal to a prime not in $\mathscr{B}$ then the ideal $(g_i(x))$ must be equal to the product of $\mathfrak{b}_i$ and a prime ideal not in $\mathfrak{B}$.

$\square$

If we are content to obtain results about 0-cycles of degree 1 instead of results about points, it would be enough to prove solubility in some field extension of each large enough degree. Arguments of this type were pioneered by Salberger. Unfortunately neither of the recipes below enables us to control either the units or the ideal class group of the field involved, so at present the usefulness of this idea is rather limited.

**Lemma 7.2.** *Let $k$ be an algebraic number field and $P_1(X), \ldots, P_n(X)$ monic irreducible non-constant polynomials in $k[X]$; and let $N \geq \sum \deg(P_i)$ be a given integer. Let $\mathfrak{B}$ be a finite set of places of $k$ which contains the infinite places, the primes at which some coefficient of some $P_i$ is not integral and any other primes $\mathfrak{p}$ at which $\prod P_i(X)$ does not remain separable when reduced mod $\mathfrak{p}$. Let $b > 1$ be in $\mathbf{Z}$ and such that no prime of $k$ which divides $b$ is in $\mathfrak{B}$. For each $v$ in $\mathfrak{B}$ let $U_v$ be a non-empty open set of separable monic polynomials of degree $N$ in $k_v[X]$. Let $M > 0$ be a fixed rational integer. Then we can find an irreducible monic polynomial $G(X)$ in $k[X]$ of degree $N$ which lies in each $U_v$ and for which $\lambda$, the image of $X$ in $K = k[X]/G(X)$, satisfies*

$$(P_i(\lambda)) = \mathfrak{P}_i \mathfrak{A}_i \mathfrak{C}_i^M \tag{14}$$

*for each $i$, where the $\mathfrak{P}_i$ are distinct first degree primes in $K$ not lying above any prime in $\mathfrak{B}$, the $\mathfrak{A}_i$ are products of bad primes in $K$ and the $\mathfrak{C}_i$ are integral ideals*

*in K. (Here we call a prime in K bad if it divides b or any prime in $\mathfrak{B}$.) Moreover we can arrange that $\lambda = \alpha/\beta$ where $\alpha$ is integral and $\beta$ is an integer all of whose prime factors are bad.*

**Lemma 7.3.** *Let k be an algebraic number field and $P_1(X), \ldots, P_n(X)$ monic irreducible non-constant polynomials in $k[X]$; and let $N \geq \sum \deg(P_i)$ be a given integer. Let $\mathfrak{B}$ be a finite set of places of k which contains the infinite places, the primes at which some coefficient of some $P_i$ is not integral and any other primes $\mathfrak{p}$ at which $\prod P_i(X)$ does not remain separable when reduced $\bmod \mathfrak{p}$.*

*Let L be a finite extension of k in which all the polynomials $P_i$ split completely, and which is Galois over $\mathbf{Q}$. Let V be an infinite set of finite primes of k lying over primes in $\mathbf{Q}$ which are totally split in L. Suppose that we are given for each $v \in \mathfrak{B}$ a non-empty open set $U_v$ of separable monic polynomials in $k_v[X]$ of degree N. Then we can find an irreducible monic polynomial G(X) in $k[X]$ of degree N such that if $\theta$ is the image of X in $k[X]/G(X)$ then*

 (i) *$\theta$ is an integer except perhaps at primes in $k(\theta)$ above those in $\mathfrak{B} \cup V$;*
 (ii) *$G(X)$ is in $U_v$ for each v in $\mathfrak{B}$;*
 (iii) *For each i there is a finite prime $w_i$ in $k(\theta)$, of absolute degree one, such that $P_i(\theta)$ is a uniformizing parameter for $w_i$ and a unit at all primes except $w_i$ and possibly some of those above some prime in $\mathfrak{B} \cup V$.*

The existence of $V$ follows from Tchebotarov's density theorem. The proof of Lemma 7.3 can be found in [52]. The proof of Lemma 7.2 is currently unpublished. The idea underlying the proofs of both these Lemmas is as follows. Write $R(X) = \prod P_i(X)$ and $R_i(X) = R(X)/P_i(X)$. Any polynomial $G(X)$ in $k[X]$ can be written in just one way in the form

$$G(X) = R(X)Q(X) + \sum R_i(X)\psi_i(X) \tag{15}$$

with $\deg \psi_i < \deg P_i$; for if $\lambda_i$ is a zero of $P_i(X)$ this is just the classical partial fractions formula

$$\frac{G(X)}{\prod P_i(X)} = Q(X) + \sum \frac{\psi_i(X)}{P_i(X)}$$

with $\psi_i(\lambda_i) = G(\lambda_i)/R_i(\lambda_i)$. This property determines for each i a unique $\psi_i(X)$ in $k[X]$ of degree less than $\deg P_i$. The same result holds over any $k_v$. If the coefficients of G are integral at v, for some v not in $\mathfrak{B}$, then so are those of Q and each $\psi_i$ because R and the $R_i$ are monic and $R_i(\lambda_i)$ is a unit outside $\mathfrak{B}$. For each v in $\mathfrak{B}$ let $G_v(X)$ be a polynomial of degree N lying in $U_v$, and write

$$G_v(X) = R(X)Q_v(X) + \sum R_i(X)\psi_{iv}(X)$$

with $\deg \psi_{iv} < \deg P_i$. We adjoin to $\mathfrak{B}$ a further finite place w at which b is a unit, and associate with it a monic irreducible polynomial $G_w(X)$ in $k_w[X]$ of degree N; the only purpose of $G_w$ is to ensure that the $G(X)$ which we construct is irreducible over k. We then build $G(X)$, close to $G_v(X)$ for every $v \in \mathfrak{B}$ including w.

Let $\mathfrak{p}_i$ be the prime in $k$ below $\mathfrak{P}_i$. By computing the resultant of $P_i(X)$ and $G(X)$ in two different ways, we obtain

$$\text{Norm}_{K/k}P_i(\lambda) = \pm\text{Norm}_{k_i/k}G(\lambda_i) = \pm\text{Norm}_{k_i/k}(\phi_i R_i(\lambda_i)) \qquad (16)$$

where $\lambda_i$ is a zero of $P_i(X)$. By hypothesis $R_i(\lambda_i)$ is a unit at every place of $k(\lambda_i)$ which does not lie above a place in $\mathfrak{B}$; and we can arrange that the denominator of $\text{Norm}_{k_i/k}\phi_i$ is only divisible by bad primes, and its numerator is the product of the first degree prime $\mathfrak{p}_i$, powers of primes in $\mathfrak{B}$ and other factors which we can largely control by the way in which we build $G(X)$. That depends on which Lemma we are trying to prove, and it is the presence of these factors that lead to the complications in the statements of the two Lemmas.

## 8   The Legendre-Jacobi Function

If $\alpha, \beta$ are elements of $k^*$ and $v$ is a place of $k$, the multiplicative *Hilbert symbol* $(\alpha, \beta)_v$ is defined by

$$(\alpha, \beta)_v = \begin{cases} 1 & \text{if } \alpha X^2 + \beta Y^2 = Z^2 \text{ is soluble in } k_v, \\ -1 & \text{otherwise.} \end{cases}$$

The additive Hilbert symbol is defined in the same way except that it takes the values 0 and 1 in $\mathbf{F}_2$ instead of 1 and $-1$. The Hilbert symbol is effectively a replacement for the quadratic residue symbol, with the advantage that it treats the even primes and the infinite places in just the same way as any other prime. It is symmetric in $\alpha, \beta$ and its principal properties are

- $(\alpha_1 \alpha_2, \beta)_v = (\alpha_1, \beta)_v (\alpha_2, \beta)_v$ and $(\alpha, \beta_1 \beta_2)_v = (\alpha, \beta_1)_v (\alpha, \beta_2)_v$;
- For fixed $\alpha, \beta$, $(\alpha, \beta)_v = 1$ for almost all $v$, and $\prod(\alpha, \beta)_v = 1$ where the product is taken over all places $v$ of $k$.

The second of these is one of the main results of class field theory.

The Legendre-Jacobi function $L$ is crucial to much of what follows. Its theory is described in some detail here, because there is no adequate source for it in print. Let $F(U,V), G(U,V)$ be homogeneous coprime square-free polynomials in $k[U,V]$. Let $\mathscr{B}$ be a finite set of places of $k$ containing the infinite places, the primes dividing 2, those at which any coefficient of $F$ or $G$ is not integral, and any primes $\mathfrak{p}$ at which $FG$ does not remain separable when reduced mod $\mathfrak{p}$.

Let $\mathscr{N}^2 = \mathscr{N}^2(k)$ be the set of $\alpha \times \beta$ with $\alpha, \beta$ integral and coprime outside $\mathscr{B}$, and let $\mathscr{N}^1 = \mathscr{N}^1(k)$ be $k \cup \{\infty\}$. For $\alpha \times \beta$ in $k \times k$ with $\alpha, \beta$ not both zero, we shall consistently write $\lambda = \alpha/\beta$ with $\lambda$ in $\mathscr{N}^1(k)$. Provided $F(\alpha, \beta)$ and $G(\alpha, \beta)$ are nonzero, we define the function

$$L(\mathscr{B}; F, G; \alpha, \beta): \ \alpha \times \beta \mapsto \prod_{\mathfrak{p}}(F(\alpha, \beta), G(\alpha, \beta))_{\mathfrak{p}} \qquad (17)$$

on $\mathcal{N}^2$, where the outer bracket on the right is the multiplicative Hilbert symbol and the product is taken over all primes $\mathfrak{p}$ of $k$ outside $\mathcal{B}$ which divide $G(\alpha,\beta)$. By the definition of $\mathcal{B}$, $F(\alpha,\beta)$ is a unit at any such prime. We can restrict the product in (17) to those $\mathfrak{p}$ which divide $G(\alpha,\beta)$ to an odd power; thus we can also write it as $\prod \chi_{\mathfrak{p}}(F(\alpha,\beta))$ where $\chi_{\mathfrak{p}}$ is the quadratic character mod $\mathfrak{p}$ and the product is taken over all $\mathfrak{p}$ outside $\mathcal{B}$ which divide $G(\alpha,\beta)$ to an odd power. This relationship with the quadratic residue symbol underlies the proof of Lemma 8.1. The function $L$ does depend on $\mathcal{B}$, but the effect on the right hand side of (17) of increasing $\mathcal{B}$ is obvious. Some of the more interesting properties of $L$ depend on $\deg F$ being even, but this usually holds in applications. In the course of the proofs, however, we need to consider functions (17) with $\deg F$ odd; and for this reason it is expedient to introduce

$$M(\mathcal{B};F,G;\alpha,\beta) = L(\mathcal{B};F,G;\alpha,\beta)(\prod(\alpha,\beta)_v)^{(\deg F)(\deg G)},$$

where the product is taken over all $\mathfrak{p}$ outside $\mathcal{B}$ which divide $\beta$ and therefore do not divide $\alpha$.

**Lemma 8.1.** *The value of M is continuous in the topology induced on $\mathcal{N}^2$ by $\mathcal{B}$. For each v in $\mathcal{B}$ there is a function $m(v;F,G;\alpha,\beta)$ with values in $\{\pm 1\}$ which is continuous on $\mathcal{N}^2$ in the v-adic topology, such that*

$$M(\mathcal{B};F,G;\alpha,\beta) = \prod_{v \in \mathcal{B}} m(v;F,G;\alpha,\beta). \tag{18}$$

*Proof.* If $\deg F$ is even, so that $M = L$, the neatest proof of the lemma is by means of the evaluation formula in [11], Lemma 7.2.4. When $\deg G$ is even but $\deg F$ may not be, the result follows from (20), and (19) then gives the general case. (The proof in [11] is for $k = \mathbf{Q}$, but there is not much difficulty in modifying it to cover all $k$.) However, the proof which we shall give, using the ideas of [53], provides a more convenient method of evaluation.

For this proof we have to impose on $\mathcal{B}$ the additional condition that it contains all primes whose absolute norm does not exceed $\deg(FG)$. As the proof in [11] shows, this condition is not needed for the truth of Lemma 8.1 itself; but we use it in the proof of (25) below, and the latter is crucial to the subsequent argument. In any case, to classify all small enough primes as bad is quite usual. We repeatedly use the fact that $L(\mathcal{B};F,G)$ and $M(\mathcal{B};F,G)$ are multiplicative in both $F$ and $G$; the effect of this is that we can reduce to the case when both $F$ and $G$ are irreducible in $\mathfrak{o}_{\mathcal{B}}[U,V]$, where $\mathfrak{o}_{\mathcal{B}}$ is the ring of elements of $k$ integral outside $\mathcal{B}$. Introducing $M$ and dropping the parity condition on $\deg F$ are not real generalizations since if we increase $\mathcal{B}$ so that the leading coefficient of $F$ is a unit outside $\mathcal{B}$ then

$$M(\mathcal{B};F,G) = L(\mathcal{B};F,GV^{\deg G}) \tag{19}$$

by (21), and we can apply (20) to the right hand side.

It follows from the product formula for the Hilbert symbol that

$$L(\mathscr{B};f,g;\alpha,\beta)L(\mathscr{B};g,f;\alpha,\beta) = \prod_{v\in\mathscr{B}}(f(\alpha,\beta),g(\alpha,\beta))_v, \qquad (20)$$

provided that $f(\alpha,\beta)$, $g(\alpha,\beta)$ are nonzero. The right hand side of (20) is the product of continuous terms each of which only depends on a single $v$ in $\mathscr{B}$. This formula enables us to interchange $F$ and $G$ when we want to, and in particular to require that $\deg F \geq \deg G$ in the reduction process which follows. We also have

$$L(\mathscr{B};f,g;\alpha,\beta) = L(\mathscr{B};f-gh,g;\alpha,\beta) \qquad (21)$$

for any homogeneous $h$ in $k[U,V]$ with $\deg h = \deg f - \deg g$ provided the coefficients of $h$ are integral outside $\mathscr{B}$, because corresponding terms in the two products are equal. Both (20) and (21) also hold for $M$.

We deal first with two special cases:

- $G$ is a constant. Now $M(\mathscr{B};F,G) = 1$ because all the prime factors of $G$ must be in $\mathscr{B}$, so that $M(\mathscr{B};F,G) = L(\mathscr{B};F,G)$ and the product in the definition of $L(\mathscr{B};F,G)$ is empty.
- $G = V$. Choose $H$ so that $F - GH = \gamma U^{\deg F}$ for some nonzero $\gamma$. Now $M(\mathscr{B};F,G) = 1$ follows from the previous case and (21), since all the prime factors of $\gamma$ must be in $\mathscr{B}$.

We now argue by induction on $\deg(FG)$. Since we can assume that $F$ and $G$ are irreducible, we need only consider the case when

$$\deg F \geq \deg G > 0, \quad G = \gamma U^{\deg G} + \dots, \quad F = \delta U^{\deg F} + \dots$$

for some nonzero $\gamma,\delta$. Let $\mathscr{B}_1$ be obtained by adjoining to $\mathscr{B}$ those primes of $k$ not in $\mathscr{B}$ at which $\gamma$ is not a unit. By (21) we have

$$M(\mathscr{B}_1;F,G) = M(\mathscr{B}_1;F-\gamma^{-1}\delta G U^{\deg F - \deg G},G). \qquad (22)$$

By taking a factor $V$ out of the middle argument on the right, and using (20), the second special case above and the induction hypothesis, we see that $M(\mathscr{B}_1;F,G)$ is continuous in the topology induced by $\mathscr{B}_1$ and is a product taken over all $v$ in $\mathscr{B}_1$ of continuous terms each one of which depends on only one of the $v$. Hence the same is true of $M(\mathscr{B};F,G)$, because this differs from $M(\mathscr{B}_1;F,G)$ by finitely many continuous factors, each of which depends only on one prime in $\mathscr{B}_1 \setminus \mathscr{B}$.

But $\mathscr{B}_1 \setminus \mathscr{B}$ only contains primes whose absolute norm is greater than $\deg(FG)$. Thus by an integral unimodular transformation from $U,V$ to $U,V_1$ we can arrange that $G = \gamma_1 U^{\deg G} + \dots$ and $F = \delta_1 U^{\deg F} + \dots$ where $\gamma_1$ is a unit at each prime in $\mathscr{B}_1 \setminus \mathscr{B}$. Let $\mathscr{B}_2$ be obtained from $\mathscr{B}$ by adjoining all the primes at which $\gamma_1$ is not a unit; then $M(\mathscr{B};F,G)$ has the same properties with respect to $\mathscr{B}_2$ that we have already shown that it has with respect to $\mathscr{B}_1$. Since $\mathscr{B}_1 \cap \mathscr{B}_2 = \mathscr{B}$, this implies that $M(\mathscr{B};F,G)$ already has these properties with respect to $\mathscr{B}$. $\square$

Of course there will be finitely many values of $\alpha/\beta$ for which at some stage of the argument the right hand side of (20) appears to be indeterminate; but by means of a preliminary linear transformation on $U, V$ one can avoid this and ensure that the formula (18) is meaningful except when $F(\alpha, \beta)$ or $G(\alpha, \beta)$ vanishes.

When $\deg F$ is even, the value of $L(\mathscr{B}; F, G; \alpha, \beta)$ is already determined by $\lambda = \alpha/\beta$ regardless of the values of $\alpha$ and $\beta$ separately; here $\lambda$ lies in $k \cup \{\infty\}$ with the roots of $F(\lambda, 1)$ and $G(\lambda, 1)$ deleted. We shall therefore also write this function as $L(\mathscr{B}; F, G; \lambda)$. But note that it is not necessarily a continuous function of $\lambda$; see the discussions in [12] and Sect. 9 of [11], or Lemma 8.4 below. Moreover if $\mathscr{B}$ does not contain a base for the ideal class group of $k$ then not all elements of $k \cup \{\infty\}$ can be written in the form $\alpha/\beta$ with $\alpha, \beta$ integers coprime outside $\mathscr{B}$; so we have not yet defined $L(\mathscr{B}; F, G; \lambda)$ for all $\lambda$. To go further in the case when $\deg F$ is even, we modify the definition (17) so that it extends to all $\alpha \times \beta$ in $k \times k$ such that $F(\alpha, \beta)$ and $G(\alpha, \beta)$ are nonzero. For any such $\alpha, \beta$ and any $\mathfrak{p}$ not in $\mathscr{B}$, choose $\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}$ integral at $\mathfrak{p}$, not both divisible by $\mathfrak{p}$ and such that $\alpha/\beta = \alpha_{\mathfrak{p}}/\beta_{\mathfrak{p}}$. Write

$$L(\mathscr{B}; F, G; \alpha, \beta) = \prod (F(\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}), G(\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}))_{\mathfrak{p}} \tag{23}$$

where the product is taken over all $\mathfrak{p}$ not in $\mathscr{B}$ such that $\mathfrak{p} | G(\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}})$. This is a finite product whose value does not depend on the choice of the $\alpha_{\mathfrak{p}}$ and $\beta_{\mathfrak{p}}$; indeed it only depends on $\lambda = \alpha/\beta$ and when $\alpha, \beta$ are integers coprime outside $\mathscr{B}$ it is the same as the function given by (17). Thus we can again write it as $L(\mathscr{B}; F, G; \lambda)$. This generalization is not really needed until we come to (27); but at that stage we cannot take account of the ideal class group of $K$ because we need $\mathscr{B}$ to be independent of $K$. Its disadvantage is that $L$ is no longer necessarily a continuous function of $\alpha \times \beta$.

If $\deg F$ or $\deg G$ is 0 or 1, it is easy to obtain an evaluation formula; so the first case of interest is when $\deg F = \deg G = 2$. Suppose that

$$F = a_1 U^2 + b_1 UV + c_1 V^2, \quad G = a_2 U^2 + b_2 UV + c_2 V^2 \tag{24}$$

and that $\mathscr{B}$ contains the infinite places and the primes which divide 2 or

$$R = (a_1 c_2 - a_2 c_1)^2 - b_1 b_2 (a_1 c_2 + a_2 c_1) + a_1 c_1 b_2^2 + a_2 c_2 b_1^2,$$

the resultant of $F$ and $G$. Suppose also that $\eta \times \zeta$ and $\rho \times \sigma$ are in $\mathscr{N}^2$. Then

$$L(\mathscr{B}; F, G; \eta, \zeta) L(\mathscr{B}; F, G; \rho, \sigma)$$
$$= \prod_{v \in \mathscr{B}} \{(f/(\sigma \eta - \rho \zeta), R)_v (fG(\rho, \sigma), -fG(\eta, \zeta))_v\}$$

where

$$f = F(\eta, \zeta) G(\rho, \sigma) - F(\rho, \sigma) G(\eta, \zeta).$$

If we set $\rho, \sigma$ to convenient values, this gives the value of $L(\mathscr{B}; F, G; \eta, \zeta)$.

The proof of Lemma 8.1 constructs an evaluation formula all of whose terms come from the right hand side of (20) for various pairs $f, g$. For $\alpha \times \beta$ in $\mathcal{N}^2$, the formula can therefore be described by an equation of the form

$$m(v; F, G; \alpha, \beta) = \prod_j (\phi_j(\alpha, \beta), \psi_j(\alpha, \beta))_v. \tag{25}$$

Here the $\phi_j, \psi_j$ are homogeneous elements of $k[U, V]$ which depend only on $F$ and $G$ and not on $v$ or $\mathcal{B}$. The decomposition (25) is not unique, but we can display an invariant aspect of it.

Let $\theta = \gamma_1 U + \gamma_2 V$ be a linear form with $\gamma_1, \gamma_2$ coprime integers in $k$. By using $(\phi, \psi)_v = (\phi, \theta \psi)_v (\phi, \theta)_v$ and $(-\theta, \theta)_v = 1$, we can ensure that all the $\phi_j, \psi_j$ in (25) have even degree except perhaps that $\psi_0 = \theta$. Denote by $\Theta$ the group of elements of $k^*$ which are not divisible to an odd power by any prime of $k$ outside $\mathcal{B}$, and by $\Theta_0 \subset \Theta$ the subgroup consisting of those $\xi$ which are quadratic residues mod $\mathfrak{p}$ for all $\mathfrak{p}$ in $\mathcal{B}$; thus we are free to multiply $\phi_0$ by any element of $\Theta_0$.

**Lemma 8.2.** *Provided* $\deg F$ *is even, if* $\psi_0 = \theta$ *we can take* $\phi_0$ *to be in* $\Theta$.

The evaluation formula for (24) shows that $(\phi_0, \psi_0)_v$ may not be trivial even when $F$ and $G$ both have even degree.

*Proof.* Let $\gamma$ in $k^*$ be a unit outside $\mathcal{B}$, and apply (25) to the identity

$$L(\mathcal{B}; F, G; \gamma \alpha, \gamma \beta) = L(\mathcal{B}; F, G; \alpha, \beta),$$

where $\alpha \times \beta$ is in $\mathcal{N}^2$. On cancelling common factors, we obtain

$$\prod_{v \in \mathcal{B}} (\phi_0(\alpha, \beta), \gamma)_v = 1. \tag{26}$$

If we can choose $\alpha \times \beta$ in $\mathcal{N}^2$ so that $\phi_0(\alpha, \beta)$ is not in $\Theta$, this gives a contradiction. For let $\delta$ prime to $\phi_0(\alpha, \beta)$ be such that $\prod(\phi_0(\alpha, \beta), \delta)_{\mathfrak{p}} = -1$ where the product is taken over all primes $\mathfrak{p}$ outside $\mathcal{B}$ at which $\phi_0(\alpha, \beta)$ is not a unit. Let $\mathcal{B}_1$ be obtained by adjoining to $\mathcal{B}$ all the primes at which $\delta$ is not a unit; then $\prod(\phi_0(\alpha, \beta), \delta)_v = -1$ by the Hilbert product formula, where the product is taken over all places $v$ in $\mathcal{B}_1$. Recalling that $\phi_0$ does not depend on $\mathcal{B}$ and writing $\mathcal{B}_1, \delta$ for $\mathcal{B}, \gamma$ in (26), we obtain a contradiction. It follows that $\phi_0(\alpha, \beta)$ lies in $\Theta$ for all $\alpha, \beta$; this can only happen if $\phi_0(U, V)$ is itself in $\Theta$ modulo squares of elements of $k[U, V]$. $\square$

In practice, what we usually need to study is the subspace of $\mathcal{N}^2$ given by $n$ conditions $L(\mathcal{B}; F_v, G_v; \alpha, \beta) = 1$, or the subspace of $\mathcal{N}^1$ given by the $L(\mathcal{B}; F_v, G_v; \lambda) = 1$, where the $\deg F_v$ are all even. Let $\Lambda$ be the abelian group of order $2^n$ whose elements are the $n$-tuples each component of which is $\pm 1$; then there is a natural identification, which we shall write $\tau$, of each element of $\Lambda$ with a partial product of the $L(\mathcal{B}; F_v, G_v)$. Thus each element of $\Lambda$ can be interpreted as a condition, which we shall write as $\mathcal{L} = 1$. If $\phi_0$ is as in Lemma 8.2, there is a homomorphism

$$\phi_0 \circ \tau : \Lambda \to \Theta/\Theta_0;$$

let $\Lambda_0$ denote its kernel. It turns out that the conditions which are continuous in $\lambda$ are just those which come from $\Lambda_0$. The following lemma corresponds to Harari's Formal Lemma (Theorem 3.2.1 of [11]); it shows that for most purposes we need only consider the conditions coming from the elements of $\Lambda_0$. For obvious reasons, we call these the *continuous* conditions.

**Lemma 8.3.** *Suppose that every* $\deg F_v$ *is even and all the conditions corresponding to* $\Lambda_0$ *hold at some given* $\lambda_0$. *Then there exists* $\lambda$ *arbitrarily close to* $\lambda_0$ *such that all the conditions* $L(\mathscr{B}; F_v, G_v) = 1$ *hold at* $\lambda$.

*Proof.* Let $\lambda_0 = \alpha_0/\beta_0$. For a suitably chosen $\gamma$ we show that we can take $\lambda = \alpha/\beta$, where $\alpha \times \beta$ is close to $\gamma\alpha_0 \times \gamma\beta_0$ at every finite prime in $\mathscr{B}$ and $\alpha/\beta$ is close to $\alpha_0/\beta_0$ at the infinite places. For any $c$ in $\Lambda$, write $\phi_{0c} = \phi_0 \circ \tau(c)$ for the corresponding element of $\Theta/\Theta_0$. If $\theta$ is as defined just before Lemma 8.2, the corresponding partial product $\mathscr{L}$ of the $L(\mathscr{B}; F_v, G_v; \lambda)$ is equal to

$$f_c(\lambda) \prod_{v \in \mathscr{B}} (\phi_{0c}, \theta(\alpha_0, \beta_0))_v \prod_{v \in \mathscr{B}} (\phi_{0c}, \gamma)_v$$

where $f_c$ comes from the $\phi_j, \psi_j$ with $j > 0$ and is therefore continuous. The map $c \mapsto f_c(\lambda)$ is a homomorphism $\Lambda \to \{\pm 1\}$ for any fixed $\lambda$; moreover if two distinct $c$ give rise to the same $\phi_{0c}$ their quotient comes from an element of $\Lambda_0$; so the quotient of the corresponding $f_c$ takes the value 1 at $\lambda_0$. In other words, if $\lambda$ is close enough to $\lambda_0$ then $f_c(\lambda)$ only depends on the class of $c$ in $\Lambda/\Lambda_0$. The map $c \mapsto \phi_{0c}$ induces an embedding $\Lambda/\Lambda_0 \to \Theta/\Theta_0$. The homomorphism $\text{Image}(\Lambda/\Lambda_0) \to \{\pm 1\}$ induced by $c \mapsto f_c(\lambda)$ can be extended to a homomorphism $\Theta/\Theta_0 \to \{\pm 1\}$ because $\Theta/\Theta_0$ is killed by 2; and any such homomorphism can be written in the form

$$\theta \to \prod_{v \in \mathscr{B}} (\theta, \gamma)_v$$

for a suitably chosen $\gamma$, because the Hilbert symbol induces a nonsingular form on $\Theta/\Theta_0$. But given any such $\gamma$ we can construct $\lambda = \alpha/\beta$ having the properties listed above.                                                                                              □

In circumstances in which we wish to use Salberger's device, we need analogues of these last statements for positive 0-cycles. To state these, we introduce more notation. We continue to assume that $\deg F$ is even. Let $K$ be the direct product of finitely many fields $k_i$ each of finite degree over $k$, and let $\mathfrak{B}$ be the set of places of $K$ lying over some place $v$ in $\mathscr{B}$, and $\mathfrak{B}_i$ the corresponding set of places of $k_i$. (The place $\prod v_i$, where $v_i$ is a place of $k_i$, lies over $v$ if each $v_i$ does so.) For $\lambda$ in $\mathbf{P}^1(K)$ write $\lambda = \prod \lambda_i$ with $\lambda_i$ in $\mathbf{P}^1(k_i)$; for each place $w$ in $k_i$ write $\lambda_i = \alpha_{iw}/\beta_{iw}$ where $\alpha_{iw}, \beta_{iw}$ are in $k_i$ and integral at $w$ and at least one of them is a unit at $w$. For any $\lambda$ in $K$ such that each $F(\lambda_i, 1)$ and $G(\lambda_i, 1)$ is nonzero, we define the function

$$L^*(\mathscr{B}; K; F, G; \lambda) : \lambda \mapsto \prod_{\mathfrak{P}_i} (F(\alpha_{iw}, \beta_{iw}), G(\alpha_{iw}, \beta_{iw}))_{\mathfrak{P}_i} \tag{27}$$

where $w$ is the place associated with the prime $\mathfrak{P}_i$ in $k_i$ and the product is taken over all $i$ and all primes $\mathfrak{P}_i$ of $k_i$ not lying in $\mathcal{B}_i$ and such that $G(\alpha_{iw}, \beta_{iw})$ is divisible by $\mathfrak{P}_i$. As with (17), we can restrict the product to those $\mathfrak{P}_i$ which divide $G(\alpha_{iw}, \beta_{iw})$ to an odd power. Note that the functions $\phi_j, \psi_j$ in the evaluation formula (25) are the same for $k_i \supset k$ as they are for $k$. Now let $\mathfrak{a}$ be a positive 0-cycle on $\mathbf{P}^1$ defined over $k$ and let $\mathfrak{a} = \cup \mathfrak{a}_i$ be its decomposition into irreducible components. Let $\lambda_i$ be a point of $\mathfrak{a}_i$ and write $k_i = k(\lambda_i)$. If $K = \prod k_i$ and $\lambda = \prod \lambda_i$, write

$$L^*(\mathcal{B}; F, G; \mathfrak{a}) = L^*(\mathcal{B}; K; F, G; \lambda) = \prod_i L(\mathcal{B}_i; F, G; \lambda_i). \tag{28}$$

This is legitimate, because the right hand side does not depend on the choice of the $\lambda_i$. If $K = k$ this $L^*$ is the same as the previous function $L$. Moreover $L^*(\mathfrak{a} \cup \mathfrak{b}) = L^*(\mathfrak{a}) L^*(\mathfrak{b})$. We can define a topology on the set of positive 0-cycles $\mathfrak{a}$ of given degree $N$ by means of the isomorphism between that set and the points on the $N$-fold symmetric power of $\mathbf{P}^1$. With this topology, it is straightforward to extend to $L^*$ the results already obtained for $L$.

The product in (27) is finite; so there is a finite set $\mathscr{S}$ of primes of $k$, disjoint from $\mathcal{B}$ and such that every $\mathfrak{P}_i$ which appears in this product lies above a prime in $\mathscr{S}$. For each $i$ we can write $\lambda_i = \alpha_i / \beta_i$ with $\alpha_i, \beta_i$ integers in $k_i$. Let $(\alpha_i, \beta_i) = \mathfrak{a}_i$ and choose an integral ideal $\mathfrak{b}_i$ in $k_i$ which is prime to $\mathfrak{a}_i$, in the same ideal class as $\mathfrak{a}_i$ and such that no prime of $k_i$ which divides $\mathfrak{b}_i$ also divides $G(\alpha_i, \beta_i)$ or any $\phi_j(\alpha_i, \beta_i)$ or $\psi_j(\alpha_i, \beta_i)$ or lies above any prime in $\mathscr{S}$. Let $\gamma_i$ be such that $(\gamma_i) = \mathfrak{b}_i / \mathfrak{a}_i$ and let $\mathcal{B}_1$ be obtained from $\mathcal{B}$ by adjoining all the primes of $k$ which lie below any prime of $k_i$ which divides $\mathfrak{b}_i$. For most purposes it costs us nothing to replace $\mathcal{B}$ by $\mathcal{B}_1$, and we then have

$$\lambda = \prod \lambda_i = \prod (\alpha_i \gamma_i / \beta_i \gamma_i) \text{ where } \alpha_i \gamma_i \times \beta_i \gamma_i \text{ is in } \mathscr{N}^2(k_i).$$

The following lemma is a trivial consequence of earlier results.

**Lemma 8.4.** *Suppose that* $\deg F$ *is even, and let* $\mathscr{L} = 1$ *be a continuous condition derived from the* $L$ *and* $\mathscr{L}^* = 1$ *the corresponding condition derived from the* $L^*$. *For each* $v$ *in* $\mathcal{B}$ *there is a function* $\ell^*(v; F, G; \mathfrak{a})$ *with values in* $\{\pm 1\}$ *which is a continuous function of* $\mathfrak{a}$ *in the* $v$*-adic topology and is such that*

$$\mathscr{L}^*(\mathcal{B}; F, G; \mathfrak{a}) = \prod_{v \in \mathcal{B}} \ell^*(v; F, G; \mathfrak{a}). \tag{29}$$

# 9  Pencils of Conics

Let $W$ be the surface fibred by the pencil of conics

$$a_0(U, V) Y_0^2 + a_1(U, V) Y_1^2 + a_2(U, V) Y_2^2 = 0. \tag{30}$$

We normally expect this pencil to be presented in a form in which $a_0, a_1, a_2$ are homogeneous of the same degree. But this is not the most convenient form for the arguments which follow. Instead we shall call the pencil *reduced* if $a_0, a_1, a_2$ are homogeneous elements of $k[U,V]$ square-free and coprime in pairs and such that

$$\deg a_0 \equiv \deg a_1 \equiv \deg a_2 \bmod 2.$$

After a linear transformation on $U, V$ if necessary, we can also assume that $a_0 a_1 a_2$ is not divisible by $V$. Clearly any pencil of conics can be put into reduced form; for if $a_i$ has a squared factor $f^2$ we write $f^{-1} Y_i$ for $Y_i$, and if for example $a_0$ and $a_1$ have a common factor $g$ we write $g Y_2$ for $Y_2$ and divide (30) by $g$. Suppose that (30) is reduced and everywhere locally soluble. Let $\lambda = \alpha/\beta$ be a point of $\mathbf{P}^1(k)$; whether (30) is soluble at $\alpha \times \beta$ depends only on $\lambda$ and not on the choice of $\alpha, \beta$. Similar statements hold for local solubility at a place $v$ and for solubility in the adeles. Let $\mathscr{B}$ be a finite set of places of $k$ containing the infinite places, the primes dividing 2, those whose absolute norm does not exceed $\deg(a_0 a_1 a_2)$, those at which any coefficient of any $a_i$ is not integral, and any other primes $\mathfrak{p}$ at which $a_0 a_1 a_2$ does not remain separable when reduced mod $\mathfrak{p}$. We also assume that $\mathscr{B}$ contains a base for the ideal class group of $k$. Denote by $c(U,V)$ an irreducible factor of $a_0 a_1 a_2$ in $k[U,V]$; we can assume that $c(U,V)$ has integer coefficients whose highest common factor is not divisible by any prime outside $\mathscr{B}$. To prove local solubility, we need only check it at the places of $\mathscr{B}$, because it is trivial at any other prime. Local solubility of (30) at the place $v$ is equivalent to $(-a_0 a_1, -a_0 a_2)_v = 1$, which can be written in the more symmetric form

$$(a_0, -a_1)_v (a_1, -a_2)_v (a_2, -a_0)_v = (-1, -1)_v. \tag{31}$$

The singular fibres of the pencil are given by the values of $\lambda$ at which $a_0 a_1 a_2$ vanishes. If there is a singular fibre defined over $k$, then (30) is certainly soluble on it; but little if any of the argument which follows makes sense there. We therefore work not on $\mathbf{P}^1$ but on the subset $\mathbf{L}^1$ obtained by deleting the zeros of $a_0 a_1 a_2$, and not on $W$ but on $W_0$, the inverse image of $\mathbf{L}^1$ in $W$. Let $\lambda \in k \cup \{\infty\}$ be a point of $\mathbf{L}^1(k)$, and write $\lambda = \alpha/\beta$ where $\alpha, \beta$ are integers of $k$ coprime outside $\mathscr{B}$; it will not matter which pair $\alpha, \beta$ we choose.

There is a non-empty set $\mathscr{N} \subset \mathbf{L}^1(k)$, open in the topology induced by $\mathscr{B}$, such that the conic (30) is soluble at every place of $\mathscr{B}$ if and only if $\lambda$ lies in $\mathscr{N}$. Let $\mathfrak{p}$ be a prime of $k$ not in $\mathscr{B}$ and consider the solubility of (30) in $k_\mathfrak{p}$ at the point $\lambda$. If none of the $a_i(\alpha, \beta)$ is divisible by $\mathfrak{p}$, then local solubility of (30) is trivial. Otherwise there is just one $c$ such that $c(\alpha, \beta)$ is divisible by $\mathfrak{p}$; to fix ideas, suppose that this $c$ divides $a_2$. The condition for local solubility at $\mathfrak{p}$ is then

$$(-a_0(\alpha, \beta) a_1(\alpha, \beta), c(\alpha, \beta))_\mathfrak{p} = 1 \tag{32}$$

where the outer bracket is the multiplicative Hilbert symbol. Hence necessary conditions for the local solubility of (30) at $\lambda$ for all $\mathfrak{p}$ outside $\mathscr{B}$ are the conditions like

$$L(\mathscr{B}; -a_0 a_1, c; \lambda) = \prod (-a_0(\alpha, \beta) a_1(\alpha, \beta), c(\alpha, \beta))_{\mathfrak{p}} = 1 \qquad (33)$$

where the product is taken over all $\mathfrak{p}$ outside $\mathscr{B}$ which divide $c(\alpha, \beta)$, and the function $L$ is well defined since $-a_0 a_1$ has even degree. There is one of these conditions for each irreducible $c$ which divides $a_0 a_1 a_2$.

What makes the set of conditions (33) interesting is that they give not merely a necessary but also a sufficient condition for solubility – at least if one assumes Schinzel's Hypothesis. In view of Lemma 8.3, it is enough to require the continuous conditions derived from the conditions (33) to hold. The following theorem provides the exact obstruction both to the Hasse principle and to weak approximation.

**Theorem 9.1.** *Assume Schinzel's Hypothesis. Let $\mathscr{A} \subset \mathscr{N}$ be the subset of $\mathbf{L}^1(k)$ at which all the continuous conditions derived from (33) hold and (30) is locally soluble at each place in $\mathscr{B}$. Then the $\lambda$ in $\mathbf{L}^1(k)$ at which (30) is soluble form a dense subset of $\mathscr{A}$ in the topology induced by $\mathscr{B}$.*

*Proof.* Let $\alpha_0 \times \beta_0$ correspond to a point $\lambda_0$ in $\mathscr{A}$, and let $\mathscr{N}_0 \subset \mathscr{A}$ be an open neighbourhood of $\lambda_0$. We have to show that we can find $\lambda_2$ in $\mathscr{N}_0$ such that (30) is soluble at $\lambda_2$; for this it is enough to show that (30) is everywhere locally soluble there. Let $c_i$ run through the factors $c$. By Lemma 8.3 we can find $\alpha_1, \beta_1$ in $k^*$, integral and coprime outside $\mathscr{B}$ and such that $\lambda_1 = \alpha_1 / \beta_1$ is in $\mathscr{N}_0$ and all the conditions (33) hold at $\alpha_1 \times \beta_1$. By Lemma 7.1 we can now find $\alpha_2 \times \beta_2$ close to $\alpha_1 \times \beta_1$ and such that each ideal $(c_i(\alpha_2, \beta_2))$ is the product of a prime ideal $\mathfrak{p}_i$ not in $\mathscr{B}$ and prime ideals in $\mathscr{B}$. We claim that (30) is everywhere locally soluble at $\alpha_2 \times \beta_2$. Since $\mathscr{N}_0 \subset \mathscr{A}$, local solubility at each place of $\mathscr{B}$ is automatic. If $\mathfrak{p}$ is a prime outside $\mathscr{B}$ which does not divide any of the $a_j(\alpha_2, \beta_2)$ then (30) at $\alpha_2 \times \beta_2$ is certainly soluble at $\mathfrak{p}$; so it only remains to consider the $\mathfrak{p}_i$. To fix ideas, suppose that $c_i(U, V)$ is a factor of $a_2(U, V)$. Taking $\alpha = \alpha_2, \beta = \beta_2$ and $c = c_i$, the product in (33) reduces to the single term with $\mathfrak{p} = \mathfrak{p}_i$. In other words, (32) holds in this case, and this proves local solubility at $\mathfrak{p}_i$. □

An apparently weaker result, but one for which it is easier to check the hypotheses, is the following. Here the hypotheses give us the existence of the $\alpha_1 \times \beta_1$ generated in the proof of Theorem 9.1, and the rest of the proof is as there. The advantage of this is that we do not need the arguments which follow (25).

**Corollary 9.2.** *Assume Schinzel's Hypothesis. Let $\mathscr{A}_1 \subset k \times k$ be the open set in which none of the $a_i$ vanish, the conditions (33) hold and (30) is locally soluble at each place in $\mathscr{B}$. Then the $\alpha \times \beta$ for which (30) is soluble form a dense subset of $\mathscr{A}_1$ in the topology induced by $\mathscr{B}$.*

The corresponding theorem for positive 0-cycles, or equivalently for 0-cycles of degree 1, does not require Schinzel's Hypothesis; instead we use Lemma 7.2 and the notation introduced at (27). We apply Lemma 7.2 to the surface $W_0$ fibred by the pencil (30), again assuming that $\mathscr{B}$ satisfies the conditions listed after (30) and that $\mathbf{L}^1$ has the same meaning as there.

**Lemma 9.3.** *With the notation above, let $N \geq \deg(a_0 a_1 a_2)$ be a fixed integer, and for each $v$ in $\mathscr{B}$ let $\mathfrak{b}'_v$ be a positive 0-cycle on $W_0$ of degree $N$ and defined over $k_v$.*

*Then we can find a positive 0-cycle $\mathfrak{a}$ of degree N on $\mathbf{L}^1$ defined over k and for each v in $\mathscr{B}$ a positive 0-cycle $\mathfrak{b}_v$ on $W_0$ of degree N and defined over $k_v$, close to $\mathfrak{b}'_v$ and such that the projection of each $\mathfrak{b}_v$ on $\mathbf{P}^1$ is $\mathfrak{a}$.*

The proof of this Lemma is a straightforward application of the Chinese Remainder Theorem. Its purpose is to show that the hypotheses of the following Theorem are less restrictive than might appear.

**Theorem 9.4.** *With the notation above, let $N \geq \deg(a_0a_1a_2)$ be a fixed integer. Let $\mathfrak{a}$ be a positive 0-cycle of degree N on $\mathbf{L}^1$ defined over k, and for each place v of k suppose that $\mathfrak{b}_v$ is a positive 0-cycle on $W_0$ of degree N and defined over $k_v$; for v in $\mathscr{B}$ suppose further that the projection of $\mathfrak{b}_v$ on $\mathbf{L}^1$ is $\mathfrak{a}$. If all the continuous conditions derived from the conditions*

$$L^*(\mathscr{B}; -a_0a_1, c; \mathfrak{a}) = 1 \tag{34}$$

*hold, then there is a positive 0-cycle of degree N on $W_0$ defined over k whose projection is arbitrarily close to $\mathfrak{a}$ in the topology induced by $\mathscr{B}$.*

*Proof.* We must first show that for the purpose of proving this theorem we are allowed to increase $\mathscr{B}$. Suppose that $\mathscr{B}_0$ satisfies the conditions which were imposed on $\mathscr{B}$ after (30), and let $\mathfrak{p}$ be a prime of k not in $\mathscr{B}_0$. Suppose also that the hypotheses of the theorem hold for $\mathscr{B} = \mathscr{B}_0$ and $\mathfrak{a} = \mathfrak{a}_0$. Having chosen $\mathfrak{b}_\mathfrak{p}$ we can find a positive 0-cycle $\mathfrak{a}'$ on $\mathbf{L}^1$ of degree N and defined over k which is close at every v in $\mathscr{B}_0$ to $\mathfrak{a}$ and close at $\mathfrak{p}$ to the projection of $\mathfrak{b}_\mathfrak{p}$. Now

$$L^*(\mathscr{B}_0 \cup \{\mathfrak{p}\}; -a_0a_1, c; \mathfrak{a}') = L^*(\mathscr{B}_0; -a_0a_1, c; \mathfrak{a}');$$

for writing both sides as products by means of (27), if there is a factor on the right hand side which is not present on the left, that factor must come from $\mathfrak{p}$ and is therefore equal to 1. But a continuous condition for $\mathscr{B}_0$ holds at $\mathfrak{a}'$ if and only if it holds at $\mathfrak{a}$, which it does by hypothesis. Hence the continuous conditions for $\mathscr{B}_0 \cup \{\mathfrak{p}\}$ hold at $\mathfrak{a}'$. Now suppose that the theorem holds for $\mathscr{B}_0 \cup \{\mathfrak{p}\}$; then there is a positive 0-cycle $\mathfrak{b}$ of degree N on $W_0$ defined over k whose projection on $\mathbf{L}^1$ is close to $\mathfrak{a}'$ in the topology induced by $\mathscr{B}_0 \cup \{\mathfrak{p}\}$. The same projection is close to $\mathfrak{a}$ in the topology induced by $\mathscr{B}_0$. So the theorem also holds for $\mathscr{B}_0$.

Note that if $\mathfrak{a}$ is actually the projection of a positive 0-cycle of degree N in $W_0$, then the continuous conditions certainly hold in view of (28); thus imposing the hypothesis that they all hold costs us nothing. To simplify the notation, we assume henceforth that K is an algebraic number field; this will be true for the application in this article because K will be constructed by means of Lemma 7.2. In view of the previous paragraph, we can assume that $\mathscr{B}$ is so large that it satisfies the conditions imposed on $\mathfrak{B}$ in the statement of Lemma 7.2 and contains the additional place w which was adjoined to $\mathfrak{B}$ in the first paragraph of the proof of Lemma 7.2; and if b is as in Lemma 7.2 we also adjoin to $\mathscr{B}$ all the primes in k which divide b. By the analogue of Lemma 8.3, we can now choose $\mathfrak{a}''$ close to $\mathfrak{a}$ so that all the conditions like $L^*(\mathscr{B}; -a_0a_1, c; \mathfrak{a}'') = 1$ hold. As was remarked in the previous paragraph, we

can now increase $\mathscr{B}$ so that if $\lambda_0 = \alpha_0/\beta_0$ is a point of $\mathbf{L}^1(K)$ in $\mathfrak{a}''$ then $\alpha_0, \beta_0$ are coprime and integral except perhaps at primes of $K$ above a prime in $\mathscr{B}$. Now apply Lemma 7.2 with $M = 2$, where we take the $c(X, 1)$, normalized to be monic, to be the $P_i(X)$ and each $U_v$ to be a small neighbourhood of the monic polynomial whose roots determine $\mathfrak{a}''$. Let $G(X)$ be given by Lemma 7.2, and let $\mathfrak{a}'$ be the associated 0-cycle on $\mathbf{L}^1(k)$ and $\lambda$ a point of $\mathbf{L}^1(K)$ in $\mathfrak{a}'$. For each $v$ in $\mathscr{B}$, the cycle $\mathfrak{a}'$ is close to $\mathfrak{a}''$ in the $v$-adic topology; so (30) at $\lambda$ is soluble in $K_w$ for each $w$ above $v$, by continuity. But $\lambda = \alpha/\beta$ with $\alpha, \beta$ coprime except at primes of $K$ above a prime of $\mathscr{B}$. So

$$\prod_{\mathfrak{P}}(-a_0(\alpha,\beta)a_1(\alpha,\beta), c(\alpha,\beta))_{\mathfrak{P}} = L^*(\mathscr{B}; -a_0 a_1, c; \alpha, \beta) = 1,$$

where the product is taken over all primes $\mathfrak{P}$ not above a prime in $\mathscr{B}$ and such that $c(\alpha, \beta)$ is divisible to an odd power by $\mathfrak{P}$. Here the first equality holds by definition and the second one follows from the evaluation formula (25) by continuity. But if $c(X, 1) = P_i(X)$ then the product on the left reduces to the single term for which $\mathfrak{P}$ is the prime of $K$ above $\mathfrak{p}_i$ whose existence was proved by means of (16). Hence (30) at $\lambda$ is locally soluble at this prime; and because these are the only primes not lying above a prime of $\mathscr{B}$ which divide any $c(\alpha, \beta)$ or any $a_i(\alpha, \beta)$ to an odd power, they are the only primes not lying above a prime of $\mathscr{B}$ at which local solubility might present any difficulty. Thus $\lambda$ can be lifted to a point of the fibre above $\lambda$, which is a conic, and the theorem now follows because weak approximation holds on conics.
□

Since (30) contains positive 0-cycles of degree 2 defined over $k$, it is trivial to deduce from Theorem 9.4 the corresponding result for 0-cycles of degree 1; conversely, if we know the analogue of Theorem 9.4 for 0-cycles of degree 1 we can deduce that (30) contains positive 0-cycles of some odd degree defined over $k$. It is tempting to hope that if a pencil of conics contains 0-cycles of degree 1 then it contains points; indeed, the corresponding result is true for Del Pezzo surfaces of degree 4, as is proved in Theorem 14.3. But this hope is false. A simple counterexample is given by the pencil

$$Y_0^2 + Y_1^2 - 7(U^2 - UV - V^2)(U^2 + UV - V^2)(U^2 - 2V^2)Y_2^2 = 0. \qquad (35)$$

This is insoluble in $\mathbf{Q}$. For we can take $\mathscr{B} = \{\infty, 2, 3, 5, 7\}$, and the three possible $c(U, V)$ are $U^2 - UV - V^2$, $U^2 + UV - V^2$ and $U^2 - 2V^2$. By (20) we have

$$L(\mathscr{B}; -1, c) = (-1, c)_\infty (-1, c)_2 (-1, c)_7,$$

the factors at 3 and 5 being trivial. Local solubility of (35) holds at each place; at $\alpha \times \beta$ local solubility at 2 and at 7 requires respectively that $4 \mid \alpha$ and $\alpha^2 - 2\beta^2$ is divisible by an odd power of 7. Hence

$$(-1, \alpha^2 \pm \alpha\beta - \beta^2)_2 = -1, \quad (-1, \alpha^2 - 2\beta^2)_2 = -1$$

and

$$(-1, \alpha^2 \pm \alpha\beta - \beta^2)_7 = 1, \quad (-1, \alpha^2 - 2\beta^2)_7 = -1.$$

To satisfy the conditions (33) we therefore need

$$(-1, \alpha^2 \pm \alpha\beta - \beta^2)_\infty = -1, \quad (-1, \alpha^2 - 2\beta^2)_\infty = 1;$$

but this is equivalent to $\alpha^2 \pm \alpha\beta - \beta^2 < 0 < \alpha^2 - 2\beta^2$, which is impossible. Now let $K = \mathbf{Q}(\rho)$ where $\rho = 2\cos(2\pi/7)$, so that $\rho^3 + \rho^2 - 2\rho - 1 = 0$. If $U = \rho^2 + 2\rho - 3$ and $V = \rho^2 + \rho - 2$ then

$$Y_0 = (\rho - 2)^2(\rho^2 - \rho + 1), \; Y_1 = (\rho - 2)^2(\rho^2 - 1), \; Y_2 = 1$$

gives a solution in $K$.

On pencils of conics the appropriate Brauer-Manin condition is a necessary and sufficient condition for the Hasse principle and for weak approximation (in each case subject to Schinzel's Hypothesis) and for the existence of positive 0-cycles of degree $N$ for all large enough $N$. This is the same as saying that the appropriate Brauer-Manin condition is equivalent to the necessary and sufficient conditions stated in Theorems 9.1 and 9.4. That is the content of the following lemma.

**Lemma 9.5.** *Let $W_0$ be everywhere locally soluble. Then the continuous conditions derived from (30) are collectively equivalent to the Brauer-Manin conditions for the existence of points of $W_0$ defined over k. The continuous conditions similarly derived from the $L^*(\mathfrak{a})$ are collectively equivalent to the Brauer-Manin conditions for the existence of positive 0-cycles of degree N on $W_0$ defined over k.*

*Proof.* The first assertion is proved for $k = \mathbf{Q}$ in [11], Sect. 8; as with Lemma 8.1, the proof there can easily be extended to our more general case. The second sentence follows trivially from the first in the light of (28).                                    □

## 10  2-Descent on Elliptic Curves

In this section we describe the process of 2-descent on elliptic curves defined over an algebraic number field $k$ which have the form

$$\Gamma : y^2 = (x - c_1)(x - c_2)(x - c_3)$$

– that is, elliptic curves all of whose 2-division points are rational. We can clearly take the $c_i$ to lie in $\mathfrak{o}$, the ring of integers of $k$. Let $\mathscr{B}$, the set of bad places, be any finite set of places containing the even primes, the infinite places, all the odd primes dividing $(c_1 - c_2)(c_1 - c_3)(c_2 - c_3)$ and a set of generators for the ideal class group of $k$; thus $\mathscr{B}$ contains the primes of bad reduction for $\Gamma$.

The basic version of 2-descent, which over $\mathbf{Q}$ goes back to Fermat, is as follows. To any point $(x, y)$ on $\Gamma(k)$ there correspond $m_1, m_2, m_3$ in $k^*$ with $m_1 m_2 m_3 = m^2 \neq 0$

such that the three equations

$$m_i y_i^2 = x - c_i \quad \text{for} \quad i = 1, 2, 3 \tag{36}$$

are simultaneously soluble. We can multiply the $m_i$ by non-zero squares; indeed we should really think of them as elements of $k^*/k^{*2}$, with a suitable interpretation of the equations which involve them. Denote by $\mathscr{C}(\mathbf{m})$ the curve given by the three equations (36), where $\mathbf{m} = (m_1, m_2, m_3)$. Looking for points of $\Gamma(k)$ is the same as looking for quadruples $x, y_1, y_2, y_3$ which satisfy (36) for some $\mathbf{m}$. If for example $\mathfrak{p}$ divides $m_1$ and $m_2$ to an odd power and therefore $m_3$ to an even power, then $x$ must be an integer at $\mathfrak{p}$ and therefore $\mathfrak{p}|(c_1 - c_2)$. Hence in looking for soluble $\mathscr{C}(\mathbf{m})$ we need only consider the finitely many $\mathbf{m}$ for which the $m_i$ are units at all primes outside $\mathscr{B}$.

One question of interest is the effect of *twisting* on the arithmetic properties of the curve $\Gamma$. If $b$ is in $k^*$, the *quadratic twist* of $\Gamma$ by $b$ is defined to be the curve

$$\Gamma_b : y^2 = (x - bc_1)(x - bc_2)(x - bc_3),$$

where we can regard $b$ as an element of $k^*/k^{*2}$. The curve $\Gamma_b$ is often written in the alternative form

$$v^2 = b(u - c_1)(u - c_2)(u - c_3).$$

The analogue of (36) for $\Gamma_b$ is

$$m_i y_i^2 = x - bc_i \quad \text{for} \quad i = 1, 2, 3;$$

we shall call the curve given by these three equations $\mathscr{C}_b(\mathbf{m})$. It is often useful to compare $\mathscr{C}(\mathbf{m})$ and $\mathscr{C}_b(\mathbf{m})$ for the same $\mathbf{m}$.

Provided one treats the $m_i$ as elements of $k^*/k^{*2}$, the triples $\mathbf{m}$ form an abelian group under componentwise multiplication:

$$\mathbf{m}' \times \mathbf{m}'' \mapsto \mathbf{m}'\mathbf{m}'' = (m_1'm_1'', m_2'm_2'', m_3'm_3'').$$

The $\mathbf{m}$ for which $\mathscr{C}(\mathbf{m})$ is everywhere locally soluble form a finite subgroup, called the 2-*Selmer group*. This is computable, and it contains the group of those $\mathbf{m}$ for which $\mathscr{C}(\mathbf{m})$ is actually soluble in $k$. This smaller group is $\Gamma(k)/2\Gamma(k)$, where $\Gamma(k)$ is the *Mordell-Weil* group of $\Gamma$. The quotient of the 2-Selmer group by this smaller group is $_2\text{Ш}$, the group of those elements of the *Tate-Safarevic group* which are killed by 2. One of the key conjectures in the subject is that the order of Ш is finite and hence a square.

The process of going from the curve $\Gamma$ to the set of curves $\mathscr{C}(\mathbf{m})$, or the finite subset which is the 2-Selmer group, is called a 2-*descent*, or sometimes a *first descent*, and the curves $\mathscr{C}(\mathbf{m})$ themselves are called 2-*coverings*. The reason for this terminology is that there is a commutative diagram

$$
\begin{array}{ccc}
\Gamma & \longrightarrow & \Gamma \\
\| & \nearrow & \\
\mathscr{C}(\mathbf{m}) & &
\end{array}
\tag{37}
$$

in which the left hand map is biregular (but defined over $\bar{k}$ rather than $k$), the top map is multiplication by 2 and the diagonal map is given by $y = m y_1 y_2 y_3$. A 2-covering which is everywhere locally soluble, and therefore in the 2-Selmer group, can also be written in the form

$$
\eta^2 = f(\xi) \quad \text{where} \quad f(\xi) = a\xi^4 + b\xi^3 + c\xi^2 + d\xi + e,
$$

and many 2-coverings do arise in this way; but a 2-covering which is not in the 2-Selmer group cannot always be put into this form.

   We now put this process into more modern language. In what follows, italic capitals will denote vector spaces over $\mathbf{F}_2$, the finite field of two elements, and each of $\mathfrak{p}$ and $\mathfrak{q}$ will be either a finite prime or an infinite place. Write

$$
Y_{\mathfrak{p}} = k_{\mathfrak{p}}^* / k_{\mathfrak{p}}^{*2}, \quad Y_{\mathscr{B}} = \oplus_{\mathfrak{p} \in \mathscr{B}} Y_{\mathfrak{p}}.
$$

Let $V_{\mathfrak{p}}$ denote the vector space of all triples $(\mu_1, \mu_2, \mu_3)$ with each $\mu_i$ in $Y_{\mathfrak{p}}$ and $\mu_1 \mu_2 \mu_3 = 1$; and write $V_{\mathscr{B}} = \oplus_{\mathfrak{p} \in \mathscr{B}} V_{\mathfrak{p}}$. This is the best way to introduce these spaces, because it preserves symmetry; but the reader should note that the prevailing custom in the literature is to define $V_{\mathfrak{p}}$ as $Y_{\mathfrak{p}} \times Y_{\mathfrak{p}}$, which is isomorphic to the $V_{\mathfrak{p}}$ defined above but not in a canonical way. Next, write $X_{\mathscr{B}} = \mathfrak{o}_{\mathscr{B}}^* / \mathfrak{o}_{\mathscr{B}}^{*2}$ where $\mathfrak{o}_{\mathscr{B}}^*$ is the group of elements of $k^*$ which are units outside $\mathscr{B}$; and let $U_{\mathscr{B}}$ be the image in $V_{\mathscr{B}}$ of the group of triples $(m_1, m_2, m_3)$ such that the $m_i$ are in $X_{\mathscr{B}}$ and $m_1 m_2 m_3 = 1$. It is known that the map $X_{\mathscr{B}} \to Y_{\mathscr{B}}$ is an embedding and $\dim U_{\mathscr{B}} = \frac{1}{2} \dim V_{\mathscr{B}}$; both these depend on the requirement that $\mathscr{B}$ contains the even primes and the infinite places, and the first of them depends also on the fact that $\mathscr{B}$ contains a base for the ideal class group. Finally, if $(x, y)$ is a point of $\Gamma(k_{\mathfrak{p}})$ other than a 2-division point then the product of the three components in the triple $(x - c_1, x - c_2, x - c_3)$ is $y^2$ which is in $k_{\mathfrak{p}}^{*2}$; so this triple has a natural image in $V_{\mathfrak{p}}$. We can supply the images of the 2-division points by continuity; for example the image of $(c_1, 0)$ is

$$
((c_1 - c_2)(c_1 - c_3), c_1 - c_2, c_1 - c_3),
\tag{38}
$$

and the image of the point at infinity is the trivial triple $(1, 1, 1)$, which is also the product of the three triples like (38). Thus we obtain a map $\Gamma(k_{\mathfrak{p}}) \to V_{\mathfrak{p}}$. This map, which is called the *Kummer map*, is a homomorphism. We denote its image by $W_{\mathfrak{p}}$; clearly $W_{\mathfrak{p}}$ is the set of those triples $\mathbf{m}$ for which (36) is soluble in $k_{\mathfrak{p}}$. The 2-Selmer group of $\Gamma$ can now be identified with $U_{\mathscr{B}} \cap W_{\mathscr{B}}$ where $W_{\mathscr{B}} = \oplus_{\mathfrak{p} \in \mathscr{B}} W_{\mathfrak{p}}$; for as was noted above, (36) is soluble at every prime outside $\mathscr{B}$ if and only if the elements of $\mathbf{m}$ are in $X_{\mathscr{B}}$.

Over the years, many people must have noticed that

$$\dim W_{\mathscr{B}} = \dim U_{\mathscr{B}} = \tfrac{1}{2}\dim V_{\mathscr{B}}. \tag{39}$$

The next major step, which explains and may well have been inspired by this relation, was taken by Tate. He introduced the bilinear form $e_{\mathfrak{p}}$ on $V_{\mathfrak{p}} \times V_{\mathfrak{p}}$, defined by

$$e_{\mathfrak{p}}(\mathbf{m}', \mathbf{m}'') = (m_1', m_1'')_{\mathfrak{p}} (m_2', m_2'')_{\mathfrak{p}} (m_3', m_3'')_{\mathfrak{p}}.$$

Here $(u, v)_{\mathfrak{p}}$ is the multiplicative Hilbert symbol already defined in Sect. 8.

The bilinear form $e_{\mathfrak{p}}$ is non-degenerate and alternating on $V_{\mathfrak{p}} \times V_{\mathfrak{p}}$, so that $e_{\mathscr{B}} = \prod_{\mathfrak{p} \in \mathscr{B}} e_{\mathfrak{p}}$ is a non-degenerate alternating bilinear form on $V_{\mathscr{B}} \times V_{\mathscr{B}}$. (For a bilinear form with values in $\{\pm 1\}$, "symmetric" and "skew-symmetric" are the same and they each mean that $e(\mathbf{m}', \mathbf{m}'') = e(\mathbf{m}'', \mathbf{m}')$; "alternating" means that also $e(\mathbf{m}, \mathbf{m}) = 1$.) It is known from class field theory that $U_{\mathscr{B}}$ is a maximal isotropic subspace of $V_{\mathscr{B}}$. Tate showed that $W_{\mathfrak{p}}$ is a maximal isotropic subspace of $V_{\mathfrak{p}}$, and therefore $W_{\mathscr{B}}$ is a maximal isotropic subspace of $V_{\mathscr{B}}$. (The proof of this, which is difficult, can be found in Milne [54].) This explains (39); and it also shows that the 2-Selmer group of $\Gamma$ can be identified with both the left and the right kernel of the restriction of $e_{\mathscr{B}}$ to $U_{\mathscr{B}} \times W_{\mathscr{B}}$.

For both aesthetic and practical reasons, one would like to show that this restriction is symmetric or skew-symmetric – these two properties being the same. But to make such a statement meaningful we need an isomorphism between $U_{\mathscr{B}}$ and $W_{\mathscr{B}}$; and though they have the same structure as vector spaces it is not obvious that there is a natural isomorphism between them. The way round this obstacle was first shown in [16]. It requires the construction inside each $V_{\mathfrak{p}}$ of a maximal isotropic subspace $K_{\mathfrak{p}}$ such that $V_{\mathscr{B}} = U_{\mathscr{B}} \oplus K_{\mathscr{B}}$ where $K_{\mathscr{B}} = \oplus_{\mathfrak{p} \in \mathscr{B}} K_{\mathfrak{p}}$. Assuming that such spaces $K_{\mathfrak{p}}$ can be constructed, let $t_{\mathscr{B}} : V_{\mathscr{B}} \to U_{\mathscr{B}}$ be the projection along $K_{\mathscr{B}}$ and write

$$U_{\mathscr{B}}' = U_{\mathscr{B}} \cap (W_{\mathscr{B}} + K_{\mathscr{B}}), \quad W_{\mathscr{B}}' = W_{\mathscr{B}} / (W_{\mathscr{B}} \cap K_{\mathscr{B}}) = \bigoplus_{\mathfrak{p} \in \mathscr{B}} W_{\mathfrak{p}}'$$

where $W_{\mathfrak{p}}' = W_{\mathfrak{p}} / (W_{\mathfrak{p}} \cap K_{\mathfrak{p}})$. The map $t_{\mathscr{B}}$ induces an isomorphism

$$\tau_{\mathscr{B}} : W_{\mathscr{B}}' \to U_{\mathscr{B}}',$$

and the bilinear function $e_{\mathscr{B}}$ induces a bilinear function

$$e_{\mathscr{B}}' : U_{\mathscr{B}}' \times W_{\mathscr{B}}' \to \{\pm 1\}.$$

The bilinear functions $U_{\mathscr{B}}' \times U_{\mathscr{B}}' \to \{\pm 1\}$ and $W_{\mathscr{B}}' \times W_{\mathscr{B}}' \to \{\pm 1\}$ defined respectively by

$$\theta_{\mathscr{B}}^{\flat} : u_1' \times u_2' \mapsto e_{\mathscr{B}}'(u_1', \tau_{\mathscr{B}}^{-1}(u_2')) \quad \text{and} \quad \theta_{\mathscr{B}}^{\sharp} : w_1' \times w_2' \mapsto e_{\mathscr{B}}'(\tau_{\mathscr{B}} w_1', w_2') \tag{40}$$

are symmetric. (For the proof, see [16].) Here the images of $w_1' \times w_2'$ under the second map and of $\tau_{\mathscr{B}} w_1' \times \tau_{\mathscr{B}} w_2'$ under the first map are the same. The 2-Selmer group of $\Gamma$ is isomorphic to both the left and the right kernel of $e_{\mathscr{B}}'$, and hence also to the kernels of the two maps (40).

There is considerable freedom in choosing the $K_{\mathfrak{p}}$, and this raises three obvious questions:

- Is there a canonical choice of the $K_{\mathfrak{p}}$?
- How small can we make $U'$ and $W'$?
- Can we ensure that the functions (40) are not merely symmetric but alternating?

These questions were first raised and also to a large extent answered in [55]; proofs of the assertions which follow can be found there. The motive for ensuring that the functions (40) are alternating is that it implies that the ranks of these functions are even; this means that their coranks, which are equal to the dimension of the 2-Selmer group, are congruent mod 2 to $\dim U_{\mathscr{B}}'$ and $\dim W_{\mathscr{B}}'$.

The answer to the first question appears to be negative, though there is little freedom in the optimum choice of the $K_{\mathfrak{p}}$ – particularly if one wishes to obtain not merely Lemma 10.1 but Theorem 10.2. Since $U_{\mathscr{B}}' \supset U_{\mathscr{B}} \cap W_{\mathscr{B}}$, the best possible answer to the second question would be that we can achieve $U_{\mathscr{B}}' = U_{\mathscr{B}} \cap W_{\mathscr{B}}$; we do this by satisfying the stronger requirement

$$W_{\mathscr{B}} = (U_{\mathscr{B}} \cap W_{\mathscr{B}}) \oplus (K_{\mathscr{B}} \cap W_{\mathscr{B}}). \tag{41}$$

For suppose that (41) holds; then $W_{\mathscr{B}} + K_{\mathscr{B}} = (U_{\mathscr{B}} \cap W_{\mathscr{B}}) + K_{\mathscr{B}}$ and it follows immediately that

$$U_{\mathscr{B}}' = U_{\mathscr{B}} \cap (W_{\mathscr{B}} + K_{\mathscr{B}}) = U_{\mathscr{B}} \cap W_{\mathscr{B}}. \tag{42}$$

The motivation for (41) is that we want to make $W_{\mathscr{B}} \cap K_{\mathscr{B}}$ as large as possible – that is, to choose $K_{\mathscr{B}}$ so that as much of it as possible is contained in $W_{\mathscr{B}}$. But because $K_{\mathscr{B}}$ must be complementary to $U_{\mathscr{B}}$, only the part of $W_{\mathscr{B}}$ which is complementary to $W_{\mathscr{B}} \cap U_{\mathscr{B}}$ is available for this purpose.

Since the 2-Selmer group $U_{\mathscr{B}} \cap W_{\mathscr{B}}$ is identified with the left and right kernels of each of the functions (40), if (42) holds then these functions are trivial and therefore alternating. The formal statement of all this is as follows.

**Lemma 10.1.** *We can choose maximal isotropic subspaces $K_{\mathfrak{p}} \subset V_{\mathfrak{p}}$ for each $\mathfrak{p}$ in $\mathscr{B}$ so that $V_{\mathscr{B}} = U_{\mathscr{B}} \oplus K_{\mathscr{B}}$. We can further ensure that*

$$W_{\mathscr{B}} = (U_{\mathscr{B}} \cap W_{\mathscr{B}}) \oplus (K_{\mathscr{B}} \cap W_{\mathscr{B}}),$$

*which implies $U_{\mathscr{B}}' = U_{\mathscr{B}} \cap W_{\mathscr{B}}$. If so, the functions $\theta_{\mathscr{B}}^{\flat}$ and $\theta_{\mathscr{B}}^{\sharp}$ defined in (40) are trivial.*

But the other properties of the $K_{\mathfrak{p}}$ chosen in this way are not at all obvious. Hence it is advantageous to consider other recipes for choosing the $K_{\mathfrak{p}}$, for which (41) does not hold but we can still prove that the functions (40) are alternating.

For this purpose we write $\mathscr{B}$ as the disjoint union of $\mathscr{B}'$ and $\mathscr{B}''$, where we shall always suppose that the even primes and the infinite places are all in $\mathscr{B}'$. For any odd prime $\mathfrak{p}$ we denote by $T_{\mathfrak{p}}$ the subset of $V_{\mathfrak{p}}$ consisting of those triples $(\mu_1, \mu_2, \mu_3)$ with $\mu_1 \mu_2 \mu_3 = 1$ for which each $\mu_i$ is in $\mathfrak{o}_{\mathfrak{p}}^*/\mathfrak{o}_{\mathfrak{p}}^{*2}$ – that is, each $\mu_i$ is the image of a $\mathfrak{p}$-adic unit. The main point of the following theorem is that for $\mathfrak{p}$ in $\mathscr{B}''$ it enables us to replace the complicated inductive definition of $K_{\mathfrak{p}}$ used in the proof of Lemma 10.1 by the much simpler choice $K_{\mathfrak{p}} = T_{\mathfrak{p}}$. How one chooses $\mathscr{B}''$ depends on the particular application which one has in mind.

**Theorem 10.2.** *Let $\mathscr{B}$ be the disjoint union of $\mathscr{B}'$ and $\mathscr{B}''$, and suppose that $\mathscr{B}'$ contains the even primes and the infinite places. We can construct maximal isotropic subspaces $K_{\mathfrak{p}} \subset V_{\mathfrak{p}}$ such that $V_{\mathscr{B}} = U_{\mathscr{B}} \oplus K_{\mathscr{B}}$,*

$$W_{\mathscr{B}'} = (U_{\mathscr{B}'} \cap W_{\mathscr{B}'}) \oplus (K_{\mathscr{B}'} \cap W_{\mathscr{B}'}) \tag{43}$$

*and $K_{\mathfrak{p}} = T_{\mathfrak{p}}$ for all $\mathfrak{p}$ in $\mathscr{B}''$; and (43) implies that $U'_{\mathscr{B}'} = U_{\mathscr{B}'} \cap W_{\mathscr{B}'}$. Moreover*

$$U'_{\mathscr{B}} = j_* U'_{\mathscr{B}'} \oplus \tau_{\mathscr{B}} W'_{\mathscr{B}''} = j_* U'_{\mathscr{B}'} \oplus \left( \oplus_{\mathfrak{p} \in \mathscr{B}''} \tau_B W'_{\mathfrak{p}} \right), \tag{44}$$

*and the restriction of $\theta_{\mathscr{B}}^{\flat}$ to $j_* U'_{\mathscr{B}'} \times j_* U'_{\mathscr{B}'}$ is trivial.*

*If $\mathscr{B}'$ also contains all the odd primes $\mathfrak{p}$ such that the $v_{\mathfrak{p}}(c_i - c_j)$ are not all congruent mod 2, then we can choose the $K_{\mathfrak{p}}$ for $\mathfrak{p}$ in $\mathscr{B}'$ so that also $\theta_{\mathscr{B}}^{\flat}$ is alternating on $U'_{\mathscr{B}}$.*

The appearance of $j_* U'_{\mathscr{B}'}$ in and just after (44) calls for some explanation. Let $u$ be any element of $U_{\mathscr{B}'}$; then $u$ is in $U_{\mathscr{B}}$. Moreover, for $\mathfrak{p}$ in $\mathscr{B}''$ the image of $u$ in $V_{\mathfrak{p}}$ is in $T_{\mathfrak{p}} = K_{\mathfrak{p}}$ and therefore in $K_{\mathfrak{p}} + W_{\mathfrak{p}}$; hence $u$ is in $U'_{\mathscr{B}}$. In this way we define a map $U'_{\mathscr{B}'} \to U'_{\mathscr{B}}$ which is clearly an injection and which we denote by $j_*$.

Lemma 10.1 is the special case of Theorem 10.2 in which $\mathscr{B}' = \mathscr{B}$ and $\mathscr{B}''$ is empty. But the proof of Lemma 10.1 is a necessary step (and indeed the most substantial step) in the proof of Theorem 10.2.

The main application of Theorem 10.2 is to twisted curves $\Gamma_b$, where we can clearly take $b$ to be an integer. Let $\mathscr{S}$ denote the set of bad primes for $\Gamma$ itself and let $\mathscr{B} \supset \mathscr{S}$ be the set of bad primes for $\Gamma_b$. If we are to apply any part of Theorem 10.2, $\mathscr{B}''$ must in practice consist entirely of primes which divide $b$ and are not in $\mathscr{S}$. To describe the effect of twisting, we shall denote by $d_b$ the dimension of the 2-Selmer group of $\Gamma_b$ regarded as a vector space over $\mathbf{F}_2$; we write $d = d_1$ for the dimension of the 2-Selmer group of $\Gamma$ itself. It is now possible to prove results about $d_b - d$, the change in the dimension of the 2-Selmer group as one goes from $\Gamma$ to $\Gamma_b$. There is reason to expect that statements about the parities of $d$ and $d_b$ will be simpler and much easier to prove than statements about their actual values. The two major statements known about $d_b$ are Lemmas 10.3 and 10.4; both of these are easy consequences of Theorem 10.2.

**Lemma 10.3.** *If $b$ is in $\mathfrak{o}_{\mathfrak{p}}^*$ for every $\mathfrak{p} \in \mathscr{S}$, then $d_b \equiv \dim(U_{\mathscr{S}} \cap W_{\mathscr{S}})$ mod 2 where $W_{\mathscr{S}} = \oplus_{\mathfrak{p} \in \mathscr{S}} W_{\mathfrak{p}}$ and the $W_{\mathfrak{p}}$ must be defined with respect to $\Gamma_b$ and not with respect to $\Gamma$. Thus $d_b$ mod 2 only depends on the classes of $b$ in the $k_{\mathfrak{p}}^*/k_{\mathfrak{p}}^{*2}$ for $\mathfrak{p}$ in $\mathscr{S}$.*

**Lemma 10.4.** *Let $\mathfrak{p}$ be an odd prime in $\mathscr{S}$ such that*

$$v_{\mathfrak{p}}(c_1 - c_2) > 0, \quad v_{\mathfrak{p}}(c_1 - c_3) = v_{\mathfrak{p}}(c_2 - c_3) = 0.$$

*Let $b$ in $k^*$ be such that $b$ is in $k_{\mathfrak{q}}^{*2}$ for all $\mathfrak{q}$ in $\mathscr{S}$ other than $\mathfrak{p}$ and $b$ is a quadratic non-residue at $\mathfrak{p}$. Then $d$ and $d_b$ have opposite parities.*

# 11  Pencils of Curves of Genus 1

In this section we shall be concerned with pencils of 2-coverings of elliptic curves defined over an algebraic number field $k$, where the underlying pencil of elliptic curves has the form

$$E: Y^2 = (X - c_1(U,V))(X - c_2(U,V))(X - c_3(U,V)). \tag{45}$$

Here the $c_i(U,V)$ are homogeneous polynomials in $\mathfrak{o}[U,V]$ all having the same even degree. By means of a linear transformation on $U,V$ we can ensure that the leading coefficients of the $c_i(U,V)$ are nonzero. Write

$$R(U,V) = p_{12}(U,V)p_{23}(U,V)p_{31}(U,V)$$

where $p_{ij} = c_i - c_j$.

The 2-coverings of (45) are given by

$$m_i(U,V)Y_i^2 = X - c_i(U,V) \text{ for } i = 1, 2, 3 \tag{46}$$

where the $m_i(U,V)$ are square-free homogeneous polynomials in $\mathfrak{o}[U,V]$ of even degree such that $m_1 m_2 m_3$ is a square. We should really regard the $m_i$ as homogeneous polynomials modulo squares, but this complicates the notation. Equation (46) are equivalent to the three equations

$$m_i Y_i^2 - m_j Y_j^2 = (c_j - c_i)Y_0^2 \tag{47}$$

of which only two are independent. The sum of two 2-coverings is obtained by multiplying the corresponding triples $\mathbf{m} = (m_1, m_2, m_3)$ componentwise and then removing squared factors. Denote by $\Gamma = \Gamma(\mathbf{m}; U, V)$ the curve given by the three equations (46) or the three equations (47) for particular values of $\mathbf{m}, U, V$, and by $C_{ij} = C_{ij}(\mathbf{m}; U, V)$ the conic given by a single equation (47). There are natural maps $\Gamma \to C_{ij}$. Equation (47) also imply

$$m_1(c_2 - c_3)Y_1^2 + m_2(c_3 - c_1)Y_2^2 + m_3(c_1 - c_2)Y_3^2 = 0, \tag{48}$$

and for $\Gamma$ to be soluble so too must be this conic. These are Brauer-Manin conditions; they do not appear explicitly in the statement of Theorem 11.2 but they are implied by the condition that $\mathcal{N}$ is not empty.

Our objective is to provide sufficient conditions for the solubility of a particular pencil of curves $\Gamma$, where the pencil is assumed to be everywhere locally soluble. We shall use a superscript 0 to denote a curve of this pencil or other objects connected with it. We shall need to distinguish between $\mathcal{S}$, the set of bad places for the pencil of curves $\Gamma$, and the larger set $\mathcal{B}$ of bad places for the particular curve $\Gamma^0(\alpha,\beta)$ on which we want to prove that there are rational points. Thus $\mathcal{S}$ is a finite set containing the infinite places, the primes above 2, those which divide the resolvent of any two coprime factors of $R(U,V)$ in $\mathfrak{o}[U,V]$ or have norm not greater than $\deg(R(U,V))$, and those which are bad in the sense of Sect. 9 for any of the pencils of conics $C_{ij}$. (In particular, this ensures that $\mathcal{S}$ contains a base for the ideal class group of $k$.) In terms of the definitions below, $\mathcal{B}$ must contain $\mathcal{S}$ and all the $\mathfrak{p}_{k\tau}$. The additional prime $\mathfrak{p}$ which we introduce at each step of the algorithm should be thought of as being thereby adjoined to $\mathcal{S}$.

We denote the irreducible factors of $p_{ij}(U,V)$ in $k[U,V]$ by $f_{k\tau}(U,V)$, and we assume that the coefficients of any $f_{k\tau}$ are integers and that there is no prime outside $\mathcal{S}$ which divides all of them. When we apply the results of Sect. 10 it will be with $U = \alpha, V = \beta$ where $\alpha \times \beta$ is so chosen that each ideal $(f_{k\tau}(\alpha,\beta))$ is the product of primes in $\mathcal{S}$ and one prime $\mathfrak{p}_{k\tau}$ outside $\mathcal{S}$; to do this we appeal to Lemma 7.1. In what follows, we shall call the $\mathfrak{p}_{k\tau}$ the *Schinzel primes*. The arguments of Sect. 10 show that we can confine ourselves to those triples $\mathbf{m}$ whose components take values in $\mathfrak{o}^*_{\mathcal{B}}$ when $U = \alpha, V = \beta$. Because of the constraint just stated on the choice of $\alpha, \beta$, this means that we can restrict the components of $\mathbf{m}$ to be products of some of the $f_{k\tau}(U,V)$ by elements of $\mathfrak{o}^*_{\mathcal{S}}$. In view of the description of 2-descents in Sect. 10, we can further restrict ourselves to the triples $\mathbf{m}$ such that $m_1 m_2 m_3$ divides $R^2$ and $m_i$ is prime to $p_{jk}$ in $k[U,V]$ up to factors in $\mathcal{S}$, where here and throughout this section $i, j, k$ is any permutation of $1, 2, 3$.

We shall also assume that the $p_{ij}(U,V)$ are coprime in $k[U,V]$. The case when this condition fails is also of interest, but the methods used and the conclusions are quite different; for a more detailed account see [56]. This assumption is weaker than that in [16], which was that $R(U,V)$ is square-free in $k[U,V]$, and it enables us to bring the example of diagonal quartics within the scope of the general theory.

The parity conditions on the degrees of the $c_i$ and $m_i$ are needed to ensure that the curves (45) and $\Gamma$ with $U = \alpha, V = \beta$ only depend on $\lambda = \alpha/\beta$ and not on $\alpha, \beta$ separately; otherwise we would not be dealing with pencils. But even if two of the $m_i$ have odd degree, which can happen if $R$ has factors of odd degree, the curve $\Gamma$ given by (46) or (47) is a 2-covering of $E$; and such 2-coverings do play a part in our arguments. For given $E$, let $G$ be the group of all triples $(m_1, m_2, m_3)$ satisfying the conditions above, including that the degrees of the $m_i$ are even, and define $G^* \supset G$ by dropping the condition that the $m_i$ have even degree. Provided we take the $m_i$ modulo squares, both $G$ and $G^*$ are finite; and either $G$ or $G^*$ can be regarded as defining those pencils of 2-coverings of the pencil $E$ which are of number-theoretic interest.

Now suppose that we are given a triple $\mathbf{m}^0 = (m_1^0, m_2^0, m_3^0)$ in $G$. Denote by $\Gamma^0 = \Gamma(\mathbf{m}^0, U, V)$ the curve of genus 1 given by the three equations (47) with $\mathbf{m} = \mathbf{m}^0$, and similarly for the $C_{ij}^0$. For simplicity we assume that the elliptic curve (45) has no primitive 4-division points defined over $k(U, V)$, and to avoid trivialities we also assume that the 2-covering $\Gamma^0$ does not correspond to a 2-division point.

The only values of $U/V$ for which $\Gamma^0$ can be soluble are ones for which $\Gamma^0$ is everywhere locally soluble; so for any such value of $U/V$ the 2-Selmer group of $E$ must contain the subgroup of order 8 generated by $\Gamma^0$ and the 2-coverings coming from the 2-division points. We shall call this the *inescapable* part of the 2-Selmer group. The essential tool in proving solubility will be the special case $p = 2$ of Lemma 4.6, which we restate for ease of reference.

**Lemma 11.1.** *Suppose that the Tate-Shafarevich group of $E/k$ is finite and the 2-Selmer group of $E$ has order 8. Then every curve representing an element of the 2-Selmer group contains rational points.*

As this shows, everything in this section will depend on the finiteness of $\mathrm{III}$; and everything will also depend on Schinzel's Hypothesis.

As in Sect. 9, we need to work not in $\mathbf{P}^1$ but in the subset $\mathbf{L}^1$ obtained by deleting the points $\lambda = \alpha/\beta$ at which $R(\alpha, \beta)$ vanishes. The topology on $\mathbf{L}^1(k)$ will be that induced by $\mathscr{S}$. There is an open set $\mathscr{N} \subset \mathbf{L}^1(k)$ such that $\Gamma^0(\alpha, \beta)$ is soluble at every place of $\mathscr{S}$ if and only if $\lambda$ lies in $\mathscr{N}$. Let us assume temporarily that we are going to apply Lemma 7.1 to choose $\alpha, \beta$ so that each ideal $(f_{k\tau}(\alpha, \beta))$ is a prime $\mathfrak{p}_{k\tau}$ up to possible (and well determined) factors in $\mathscr{S}$. Until we have chosen $\alpha, \beta$ we do not know the $\mathfrak{p}_{k\tau}$; but we do already know a set of generators of $U_\mathscr{B}$ as polynomials in $U, V$, and in the notation of Sect. 10 we also know the bilinear form $e_\mathscr{B}$ because of the results of Sect. 8. It is therefore possible to implement all the apparatus of Sect. 10. Solubility of $\Gamma^0(\alpha, \beta)$ at a particular Schinzel prime $\mathfrak{p}_{k\tau}$ is equivalent to the bilinear form $e_\mathscr{B}$ defined in Sect. 10 taking the value 1 at each $\mathbf{m}^0 \times w$, where $w$ is either of the two generators of $W$ associated with $\mathfrak{p}_{k\tau}$. This is a Legendre-Jacobi condition, so it determines a certain open set $\mathscr{N}_\mathfrak{p} \subset \mathbf{L}^1(k)$ where $\mathfrak{p} = \mathfrak{p}_{k\tau}$. If we take any $\alpha/\beta$ not in $\mathscr{N}_\mathfrak{p}$ and make no assumption about $f_{k\tau}(\alpha, \beta)$, then $\prod e_\mathscr{B}(\mathbf{m}^0, w)$ taken over the $w$ coming from the prime factors of $f_{k\tau}(\alpha, \beta)$ not in $\mathscr{S}$ will be the same Legendre-Jacobi function which we have just studied and will therefore have the same value $-1$. In other words, $\Gamma^0(\alpha, \beta)$ will be locally insoluble at some prime dividing $f_{k\tau}(\alpha, \beta)$. Thus for studying the solubility of (46) we can replace $\mathscr{N}$ by the intersection of $\mathscr{N}$ with all the $\mathscr{N}_\mathfrak{p}$. In what follows we assume that this new $\mathscr{N}$ is not empty.

In contrast to what happened in Sect. 9, nothing is gained by simply applying Lemma 7.1 to choose $\alpha, \beta$ so that all the $f_{k\tau}(\alpha, \beta)$ are prime up to possible factors in $\mathscr{S}$, because this might give rise to a 2-Selmer group too big for us to be able to apply Lemma 11.1. What we do instead is most conveniently described as an algorithm, which consists of repeatedly introducing a further well-chosen prime $\mathfrak{p}$ into $\mathscr{S}$, with a corresponding extra condition on the set $\mathscr{N}$ of possible values of $U \times V$, in such a way that if we then apply Lemma 7.1 the dimension of the 2-Selmer group is one less than it would have been before. If we can go on doing this as long as

the 2-Selmer group remains too big, we shall eventually reach a situation to which we can apply Lemma 11.1. However, this process cannot be always possible; for otherwise we would be able to prove that the Hasse principle held for the pencil (46), and this is known to be false. Hence there must be a potential obstruction to the argument. This is provided by Condition D, which will be introduced below. What we thereby obtain is Theorem 11.2 below.

The process of introducing a new prime $\mathfrak{p}$ is as follows. We choose an $f_{k\tau}$ and integers $\theta_{\mathfrak{p}}, \phi_{\mathfrak{p}}$ not both divisible by $\mathfrak{p}$ and such that $\mathfrak{p} \| f_{k\tau}(\theta_{\mathfrak{p}}, \phi_{\mathfrak{p}})$. Without loss of generality we can assume that $\theta_{\mathfrak{p}}, \phi_{\mathfrak{p}}$ are coprime. Choose integers $\gamma_{\mathfrak{p}}, \delta_{\mathfrak{p}}$ such that $\theta_{\mathfrak{p}} \delta_{\mathfrak{p}} - \phi_{\mathfrak{p}} \gamma_{\mathfrak{p}} = 1$, write

$$U = \theta_{\mathfrak{p}} U_1 + \gamma_{\mathfrak{p}} V_1, \quad V = \phi_{\mathfrak{p}} U_1 + \delta_{\mathfrak{p}} V_1$$

and impose on $\mathcal{N}$ the additional condition $\mathfrak{p}^2 | V_1$. Thus at any point of $\mathcal{N}$ the value of $f_{k\tau}$ is exactly divisible by $\mathfrak{p}$, and the values of all the other functions $f_{..}$ are prime to $\mathfrak{p}$.

For given $f_{k\tau}$ which $\mathfrak{p}$ satisfy the condition that there exist $\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}$ as above? Let $K_{k\tau} = k[X]/f_{k\tau}(X,1)$ be the field obtained by adjoining to $k$ a root of $f_{k\tau}$, and let $\xi_{k\tau}$ be the class of $X$ in $K_{k\tau}$; thus $f_{k\tau}(\xi_{k\tau}, 1) = 0$. The singular fibres of the pencil of elliptic curves (45), as also those of the pencil of 2-coverings (46), correspond to the roots of the $f_{k\tau}$. The reason for being interested in the singular fibres is as follows. Let $\mathfrak{p}$ be a prime of $k$ not in $\mathscr{S}$, and let $\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}$ in $\mathfrak{o}$ be such that $\mathfrak{p} \| f_{k\tau}(\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}})$; such $\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}$ exist if and only if there is a prime $\mathfrak{P}$ in $K_{k\tau}$ whose relative norm over $k$ is $\mathfrak{p}$. This last condition may appear tiresome. But what one really does is to choose a first-degree prime $\mathfrak{P}$ in $K_{k\tau}$ and define $\mathfrak{p}$ to be the prime below it in $k$. Now norm $\mathfrak{P} = \mathfrak{p}$ is automatic.

The arguments needed to validate each step of the algorithm are lengthy, and we list them as (i)–(v) below. We impose further conditions on the additional prime $\mathfrak{p}$ which ensure (i); we then deduce (ii), (iii) and (iv). Finally we use Condition D to show that unless the process is complete, we can choose $\mathfrak{p}$ so that (v) holds. After all this we choose $\alpha \times \beta$ according to the recipe in Lemma 7.1 for the $f_{k\tau}$, and with the additional property that $L(\mathscr{S}; U, V; \alpha, \beta) = 1$ if there is any $f_{k\tau}$ of odd degree. One can satisfy this additional requirement by a slight modification of the construction used to prove Lemma 7.1. Alternatively, one can render it unnecessary by replacing $U, V$ by homogeneous quadratic forms in $U_1, V_1$; this does not alter the values of the functions $L$.

 (i)  We determine necessary and sufficient conditions for $\Gamma(\alpha, \beta)$ to be locally soluble at $\mathfrak{p}$. We use these immediately to choose $\mathfrak{p}$-adic conditions on $\mathcal{N}$ such that $\Gamma^0(\alpha, \beta)$ is locally soluble at $\mathfrak{p}$; but in (v) we shall also need them to ensure for a particular $\mathbf{m}$ that the corresponding $\Gamma(\alpha, \beta)$ is not locally soluble at $\mathfrak{p}$.

For (ii)–(iv) we assume that $\alpha \times \beta$ satisfies the conditions of Lemma 7.1.

 (ii) The bilinear form $\theta_{\mathscr{B}}^{\sharp} : W_{\mathscr{B}}' \times W_{\mathscr{B}}' \to \{\pm 1\}$ defined in (40) does not depend on the choice of $\alpha \times \beta$ and hence of the $\mathfrak{p}_{k\tau}$.

By this we mean that if we change $\alpha, \beta$, thereby replacing the old $W'$ by a new $W'$ canonically isomorphic to it and replacing the old $\mathfrak{p}_{k\tau}$ in $\mathscr{B}$ by the new ones, then this isomorphism preserves $\theta_{\mathscr{B}}^\sharp$. The next result which we need, which is only meaningful once we have proved (ii), is as follows:

(iii)  We determine the effect on the function $\theta_{\mathscr{B}}^\sharp$ of introducing a new prime $\mathfrak{p}$ in the way described above.
(iv)  The curve $\Gamma^0(\alpha, \beta)$ is locally soluble at $\mathfrak{p}_{k\tau}$.

By requiring that $\lambda = \alpha/\beta$ is in $\mathscr{N}$ we ensure that $\Gamma^0(\alpha, \beta)$ is soluble in $k_v$ for every $v$ in $\mathscr{S}$ including $\mathfrak{p}$; and it is also soluble at all the Schinzel primes other than possibly $\mathfrak{p}_{k\tau}$. Thus (i) and (iv) prove that the class of $\Gamma^0(\alpha, \beta)$ is in the 2-Selmer group of the curve $E(\alpha, \beta)$ given by (45) provided that $\alpha, \beta$ are chosen according to the recipe in Lemma 7.1. The $\mathfrak{p}_{k\tau}$ are not determined until we know $\alpha$ and $\beta$; but this is unimportant because of (ii). Finally, the condition which we need for our algorithm to achieve what we want is as follows:

(v)  If $\mathbf{m}$ is in the kernel of the old $\theta_{\mathscr{B}}^\sharp$ but not in the inescapable part of it, then we can introduce a new prime $\mathfrak{p}$ which removes $\mathbf{m}$ from the kernel and does not put anything new into it.

It is in the proof of (v) that we need Condition D. Once we have (v), we can after a sufficient number of steps satisfy the conditions of Lemma 11.1, and this implies that $\Gamma^0(\alpha, \beta)$ has rational solutions. The result of this process is Theorem 11.2. A more sophisticated treatment of the solubility of pencils (46) can be found in Chap. I of [14].

**Theorem 11.2.** *Assume Schinzel's Hypothesis and the finiteness of* Ш*, and suppose that the three $p_{ij}(U,V)$ are coprime in $k[U,V]$. Suppose that the $\mathscr{N}$ constructed above is not empty and that Condition D holds. Then we can construct a non-empty set $\mathscr{A}$ which lies in the closure of the set of $\lambda$ in $\mathbf{L}^1(k)$ at which $\Gamma^0(\alpha, \beta)$ is soluble in k.*

Theorem 11.2 gives a sufficient condition for the Hasse principle to hold, though the condition is not always necessary. Indeed, we shall see at the end of this section that we can replace Condition D by a potentially weaker Condition E; but probably even the latter is not always necessary for solubility. The relation between Condition D and the Brauer-Manin obstructions is addressed in [16].

*Achieving* (i). The condition that any particular $\Gamma$ is soluble in $k_{\mathfrak{p}}$ throughout some neighbourhood of $\alpha_{\mathfrak{p}} \times \beta_{\mathfrak{p}}$ is that the reduction of $\Gamma(\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}})$ mod $\mathfrak{p}$ should contain a point defined over $\mathfrak{o}/\mathfrak{p}$ which is liftable to a point on $\Gamma$ defined over $k_{\mathfrak{p}}$. Denote by $L_{k\tau}$ the least extension of $K_{k\tau}$ over which some absolutely irreducible component of the singular fibre at $\xi_{k\tau} \times 1$ is defined; conveniently, all these components are defined over the same least extension, which is normal over $K_{k\tau}$. The decomposition of $\Gamma(\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}})$ mod $\mathfrak{p}$ corresponds to the decomposition of the fibre $\Gamma(\xi_{k\tau}, 1)$; so we can solve $\Gamma$ in $k_{\mathfrak{p}}$ in a suitable neighbourhood of $\alpha_{\mathfrak{p}} \times \beta_{\mathfrak{p}}$ if and only if $\mathfrak{P}$ splits completely in $L_{k\tau}$.

If $f_{k\tau} \| p_{ij}$, each singular fibre given by $f_{k\tau} = 0$ of the pencil of curves $\Gamma$ splits as a pair of irreducible conics which meet in two points and are each defined over the field $L_{k\tau} = K_{k\tau}(\sqrt{g_{k\tau}(\xi_{k\tau}, 1)})$; here $g_{k\tau} = m_k$ if $f_{k\tau}$ divides neither of $m_i$ and $m_j$ or $g_{k\tau} = m_k p_{jk}$ if $f_{k\tau}$ divides both of them. The same holds if $f_{k\tau}^2 | p_{ij}$ and $f_{k\tau}$ divides neither $m_i$ nor $m_j$, and again we have $g_{k\tau} = m_k$. If $f_{k\tau}^2 | p_{ij}$ and $f_{k\tau}$ divides both $m_i$ and $m_j$, then each singular fibre given by $f_{k\tau} = 0$ splits as a set of four lines which form a skew quadrilateral, and each of these lines is defined over

$$ L_{k\tau} = K_{k\tau} \left( \sqrt{m_k(\xi_{k\tau}, 1)}, \sqrt{p_{jk}(\xi_{k\tau}, 1)} \right). \tag{49} $$

Write $L_{k\tau}^0$ for the field corresponding to $\Gamma^0$ under this construction. To test for Condition D, we need to list those $\mathbf{m}$ for which $L_{k\tau}$ is contained in $L_{k\tau}^0$. It is easy to verify that they form a group, which contains $m^0$ and the triples coming from the 2-division points.

*Proof of* (ii). We are allowed to choose $\alpha \times \beta$ only within a set which is small in the topology induced by $\mathscr{S}$. In particular, this means that the power of any prime in $\mathscr{S}$ which divides any $f_{k\tau}(\alpha, \beta)$ is independent of $\alpha$ and $\beta$. Since the only other prime which divides any particular $f_{k\tau}(\alpha, \beta)$ is $\mathfrak{p}_{k\tau}$, which does so to the first power, the ideal class of $\mathfrak{p}_{k\tau}$ is fixed. If the place $v$ is given by some $\mathfrak{p}_{k\tau}$ then a generator of $W_v'$ can be lifted back to $\sigma \times \tau$ where each of $\sigma$ and $\tau$ is either 1 or $f_{k\tau}(\alpha, \beta)$; and if $v$ is in $\mathscr{S}$ the elements of a base for $W_v'$ can be lifted back to elements $\sigma \times \tau$ independent of $\alpha, \beta$ with $\sigma, \tau$ in $\mathfrak{o}_{\mathscr{S}}^*$. We choose a base for $W_{\mathscr{B}}'$ composed of these two kinds of elements; then the value of $\theta_{\mathscr{B}}^{\sharp}$ at any pair of elements of this base is a product of expressions of the form $(\sigma'(\alpha, \beta), \tau'(\alpha, \beta))_v$ where $v$ is in $\mathscr{B}$ and each of $\sigma'$ and $\tau'$ is the product of an element of $\mathfrak{o}_{\mathscr{S}}^*$ and possibly an $f_{k\tau}$. If $v$ is in $\mathscr{S}$ the value of this expression is independent of $\alpha, \beta$. If $v$ is given by $\mathfrak{p}_{k\tau}$ then using symmetry and $(\xi, -\xi)_v = 1$ if necessary we can reduce to the case when $\sigma'$ is not divisible by $f_{k\tau}$. If also $\tau'$ is not divisible by $f_{k\tau}$ then $(\sigma'(\alpha, \beta), \tau'(\alpha, \beta))_v = 1$; otherwise $(\sigma'(\alpha, \beta), \tau'(\alpha, \beta))_v = L(\mathscr{S}; \sigma', \tau'; \alpha, \beta)$ is continuous.

*Achieving* (iii). When we introduce $\mathfrak{p}$ we adjoin two more generators to $W$, and the description in terms of $U, V$ of the product of $\mathfrak{p}$ and the new $\mathfrak{p}_{k\tau}$ is the same as the description of the old $\mathfrak{p}_{k\tau}$. We use Theorem 10.2 with $\mathscr{B}'' = \{\mathfrak{p}, \mathfrak{p}_{k\tau}\}$ to describe the change in $W'$. In the notation of Sect. 10 all the triples in $W_{\mathfrak{p}}$ have $v_{\mathfrak{p}}(m_k)$ even. Since $K_{\mathfrak{p}} = T_{\mathfrak{p}}$, the set of triples all whose components are units at $\mathfrak{p}$, it follows that $W_{\mathfrak{p}} \cap K_{\mathfrak{p}}$ has dimension 1 and so has $W_{\mathfrak{p}}'$. A similar argument holds for the primes $\mathfrak{p}_{k\tau}$ provided by Lemma 7.1, and shows that to each such prime there corresponds one generator of $W'$. Hence introducing $\mathfrak{p}$ increases the dimension of $W'$ by 1. If we regard the $\theta^{\sharp}$ defined at (40) as being given by a matrix whose last two columns are the only ones which depend on $\mathfrak{p}_{k\tau}, \mathfrak{p}$ respectively, the old $\theta^{\sharp}$ can be obtained from the new one by adding together the last two rows and the last two columns.

*Proof of* (iv). As we have just noted,

$$ e^*(\mathbf{m}^0, w^{\text{old}}) = e^*(\mathbf{m}^0, w_{\mathfrak{p}}) e^*(\mathbf{m}^0, w^{\text{new}}) $$

where $w^{\text{old}}$ and $w^{\text{new}}$ correspond to the old and the new $\mathfrak{p}_{k\tau}$. The first two factors here are 1, so the third must be so.

*Choice of* $\mathfrak{p}$. Let $w_{\mathfrak{p}}$ be a lift to $W_{\mathfrak{p}}$ of the non-trivial element of $W'_{\mathfrak{p}}$, and let $\mathbf{m}$ be an element of $U_{\mathscr{B}} \cap W_{\mathscr{B}}$ which is not in the inescapable part of the 2-Selmer group. Thus $\tau_{\mathscr{B}}^{-1}\mathbf{m}$ is in the kernel of $e^*_{\mathscr{B}}$. Suppose that we can choose $\mathfrak{p}$ so that the 2-covering corresponding to $\mathbf{m}$ is locally insoluble at $\mathfrak{p}$. On the one hand this is equivalent to $e^*(\tau_{\mathscr{B}}^{-1}\mathbf{m}, w_{\mathfrak{p}}) = -1$. On the other hand it requires $\mathfrak{P}$ to split completely in $L^0_{k\tau}$ but not in $L_{k\tau}$. The condition below, which in the literature is called Condition D, ensures that such a choice is possible. We shall see later that Condition D can be replaced by a weaker condition, but one which is less natural and sometimes less computationally convenient.

Condition D: *If* $\mathbf{m}$ *is not in the inescapable subgroup of the 2-Selmer group, then there is a pair* $k, \tau$ *such that the field* $L_{k\tau}$ *is not contained in* $L^0_{k\tau}$.

By incorporating the definitions of $L_{k\tau}$ and $L^0_{k\tau}$ into this condition, we can restate it as follows:

*The kernel of the composite map*

$$\mathbf{m} \mapsto \oplus_{k,\tau} g_{k\tau}(\mathbf{m}) \mapsto \oplus_{k,\tau} K^*_{k\tau}/\langle K^{*2}_{k\tau}, H_{k\tau}\rangle$$

*is generated by the inescapable subgroup of the* 2-*Selmer group, where*

$$g_{k\tau} = \begin{cases} m_k & \text{if } f_k \text{ divides neither of } m_i \text{ and } m_j, \\ m_k p_{jk} & \text{if } f_k \text{ divides both of } m_i \text{ and } m_j, \end{cases}$$

*and*

$$H_{k\tau} = \begin{cases} m_k(\xi_{k\tau}, 1) & \text{if } f_{k\tau} \text{ divides neither of } m_i \text{ and } m_j, \\ m_k(\xi_{k\tau}, 1)p_{jk}(\xi_{k\tau}, 1) & \text{if } f_{k\tau} \| p_{ij} \text{ and } f_{k\tau} \text{ divides } m_i \text{ and } m_j, \\ \{m_k(\xi_{k\tau}, 1), p_{jk}(\xi_{k\tau}, 1)\} & \text{if } f^2_{k\tau} \| p_{ij} \text{ and } f_{k\tau} \text{ divides } m_i \text{ and } m_j. \end{cases}$$

The $\mathbf{m}$ for which $L_{k\tau}$ is contained in $L^0_{k\tau}$ for each subscript $k\tau$ are those which do not satisfy Condition D. If $\mathbf{m}$ satisfies Condition D we can choose $k, \tau$ and a $\mathfrak{P}$ which splits in $L^0_{k\tau}$ but not in $L_{k\tau}$. The underlying $\mathfrak{p}$ has the properties we want. This process remove $\mathbf{m}$ from the 2-Selmer group without creating any new elements of that group. So we have certainly decreased the dimension of the 2-Selmer group, which is what we needed to show to justify the algorithm. In fact it is easy to show that we have decreased it by exactly 1.

It will be seen that we have not used the full force of Condition D; indeed it is stated for all elements of $G^*$, but we have only used it for those elements which lie in the initial 2-Selmer group. These are the ones for which the corresponding 2-covering is locally soluble at each place in $\mathscr{B}$. The proof of (ii) above shows that local solubility in $\mathscr{S}$ implies local solubility at each $\mathfrak{p}_{k\tau}$; and the proof of (iii) shows that this 2-Selmer group, considered as a subgroup of $G^*$, does not vary as $\alpha \times \beta$ varies within a small enough open set. We actually use Condition D only for the $\mathbf{m}$ which lie in this 2-Selmer group; and to require merely that such $\mathbf{m}$ satisfy Condition D is weaker than the full Condition D. We call this weaker condition Condition

E. Its disadvantage is that Condition D is independent of $\alpha$ and $\beta$, whereas Condition E is not; however Condition E becomes independent of $\alpha \times \beta$ when $\alpha \times \beta$ is restricted to a small enough open set. A particularly favourable case is when the 2-Selmer group has order 8, because then Condition E is trivial. I do not know whether Condition E, together with the conditions imposed in Theorem 11.2, is necessary as well as sufficient for global solubility, nor whether these conditions are together equivalent to the Brauer-Manin conditions, though I doubt whether either of these is true. However, the arguments in [11] do enable one to link Conditions D and E to the Brauer-Manin obstructions.

## 12   Some Examples

In this section we consider three particular families of surfaces to which the ideas of the previous section (suitably modified in the last two examples) can be applied. The first family consists of diagonal quartic surfaces (51), subject to the additional condition (52) which ensures that (51) contains a pencil of curves of genus 1 whose Jacobian has rational 2-division points. The second family is a particular family of Kummer surfaces, and the third consists of diagonal cubic surfaces. What these last two examples have in common is that the argument does not use Schinzel's Hypothesis; more precisely, we only need to force one linear polynomial to take a prime value, and this can be done by means of Dirichlet's Theorem on primes in arithmetic progression. But the price of this is that we have to apply Lemma 4.6 to two pencils of elliptic curves rather than to one, and to make the process work the constraints on the choice of additional primes associated with the two pencils must not interfere with each other. Thus the proof requires some additional (but not very restrictive) conditions which are unlikely to be actually needed for solubility. For the third example we also need to require that the field $k$ over which we work does not contain $\sqrt{-3}$.

### 12.1   Diagonal Quartic Surfaces

Let $V$ be a smooth quartic surface whose equation can be put into the form $AD = BC$, where $A, \ldots, D$ are linearly independent homogeneous quadratics in $X_0, \ldots, X_3$. Such a $V$ is fibred by the pencil of curves of genus 1

$$yA = zB, \quad yC = zD, \tag{50}$$

which are 2-coverings of elliptic curves. Recall that if $M_1, M_2$ are the matrices associated with the quadratic forms $yA - zB$ and $yC - zD$ respectively, then the Jacobian of (50) can be written in the form $Y^2 = f(Z)$ where $f$ is the resolving cubic of the quartic polynomial $\det(M_1 - XM_2)$. Hence if $A, \ldots, D$ are linear combinations of

the $X_i^2$ then the 2-division points of the Jacobian of (50) are all rational. Over an algebraic number field $k$ the K3 surfaces whose equations have the form

$$a_0 X_0^4 + a_1 X_1^4 + a_2 X_2^4 + a_3 X_3^4 = 0 \tag{51}$$

satisfy the condition above if and only if

$$a_0 a_1 a_2 a_3 \text{ is a square.} \tag{52}$$

Full details of the argument which follows can be found in [17]. We shall always assume that (51) is everywhere locally soluble and the $a_i$ are integral. The surfaces (51) are very special within the family of nonsingular quartic surfaces for at least two reasons: they are Kummer surfaces, and their Néron-Severi groups over **C** have maximal rank, which is 20. But this is probably the simplest family of K3 surfaces that can be written down explicitly.

It is known that the Néron-Severi group of (51) over **C** is generated by the 48 lines on the surface. However, what is equally important for our purposes is the Néron-Severi group over $k$. When $k = \mathbf{Q}$ there are now 282 possibilities for the Galois group over **Q** of the least field of definition of the 48 lines; these have been tabulated by Martin Bright in his Cambridge Ph.D. thesis [57], which can be found at

http://www.boojum.org.uk/maths/quartic-surfaces/

together with a good deal of other relevent material. The large number of cases means that the calculation needed to be automated, and one interesting feature of the thesis is that it shows that this is possible.

Write $A = \alpha_0 X_0^2 + \alpha_1 X_1^2 + \alpha_2 X_2^2 + \alpha_3 X_3^2$ and so on. Eliminating each of the four variables $X_v$ from (50) in turn, we obtain four equations of the form

$$d_{i\ell} X_i^2 + d_{j\ell} X_j^2 + d_{k\ell} X_k^2 = 0, \tag{53}$$

only two of which are linearly independent. Here $i, j, k, \ell$ is any permutation of $1, 2, 3, 4$ and $d_{\mu v}$ is the value of the determinant formed by columns $\mu$ and $v$ of the matrix

$$\begin{pmatrix} \alpha_0 y - \beta_0 z & \alpha_1 y - \beta_1 z & \alpha_2 y - \beta_2 z & \alpha_3 y - \beta_3 z \\ \gamma_0 y - \delta_0 z & \gamma_1 y - \delta_1 z & \gamma_2 y - \delta_2 z & \gamma_3 y - \delta_3 z \end{pmatrix}.$$

We have the unexpected result that each $d_{k\ell}$ is a constant multiple of $d_{ij}$, where $i, j, k, \ell$ is any permutation of $0, 1, 2, 3$. We note the identity

$$d_{01} d_{23} + d_{02} d_{31} + d_{03} d_{12} = 0,$$

which is frequently useful. The Jacobian of the curve (50) has the form

$$E : Y^2 = (X - c_1)(X - c_2)(X - c_3)$$

where
$$c_1 - c_2 = d_{03}d_{21}, \quad c_2 - c_3 = d_{01}d_{32}, \quad c_3 - c_1 = d_{02}d_{13},$$

and the map from the curve (50) to its Jacobian is given by

$$Y = d_{12}d_{23}d_{31}X_1X_2X_3/X_0^3, \quad X - c_i = d_{ij}d_{ki}X_i^2/X_0^2$$

where $i, j, k$ is any permutation of $1, 2, 3$. Although everything so far is homogeneous in $y, z$, we have to work in $k(y,z)$ rather than $k(y/z)$, for reasons which are already implicit in Sect. 8.

There is an obvious map from (51) to the quadric surface

$$a_0Y_0^2 + a_1Y_1^2 + a_2Y_2^2 + a_3Y_3^2 = 0. \tag{54}$$

We have assumed that (51), and therefore (54), is everywhere locally soluble; so (54) is soluble in $k$. From this and the fact that $a_0a_1a_2a_3$ is a square it follows that $-a_1$ is represented by $a_2Y_2^2 + a_3Y_3^2$ over $k$. In other words, there exist integers $r_1, r_2, r_3$ and $h$ such that
$$a_1r_1^2 + a_2r_2^2 + a_3r_3^2 = 0, \quad h^2 = a_0a_1a_2a_3.$$

After rescaling (51) if necessary, we can take

$$\begin{aligned}
A(X^2) &= hr_2X_0^2 + a_1a_3(r_3X_1^2 - r_1X_3^2), \\
B(X^2) &= hr_3X_0^2 - a_1a_2(r_2X_1^2 + r_1X_2^2), \\
C(X^2) &= a_3hr_3X_0^2 - a_1a_2a_3(r_2X_1^2 - r_1X_2^2), \\
D(X^2) &= -a_2hr_2X_0^2 - a_1a_2a_3(r_3X_1^2 + r_1X_3^2);
\end{aligned}$$

and the $d_{ij}$ are given by

$$\begin{aligned}
d_{23} &= a_1^2a_2a_3r_1^2(a_3y^2 + a_2z^2), \quad d_{01} = (h/a_2a_3)d_{23}, \\
d_{31} &= a_1^2a_2a_3r_1(a_3r_2y^2 - 2a_3r_3yz - a_2r_2z^2), \quad d_{02} = (h/a_3a_1)d_{31}, \\
d_{12} &= a_1^2a_2a_3r_1(a_3r_3y^2 + 2a_2r_2yz - a_2r_3z^2), \quad d_{03} = (h/a_1a_2)d_{12}.
\end{aligned}$$

These choices do not preserve the symmetry, but that loss appears to be unavoidable. Changing the $r_i$ corresponds to a linear transformation on $y, z$; changing the sign of $h$ gives the pencil $yA = zC, yB = zD$ instead of (50).

The 2-covering of $E$ given by the triple $(m_1, m_2, m_3)$ with $m_1m_2m_3 = 1$ is

$$m_iZ_i^2 = X - c_i \text{ for } i = 1, 2, 3 \quad \text{and} \quad Y^2 = Z_1Z_2Z_3.$$

As in Sect. 11, values associated with the particular 2-covering given by (50) will be denoted by a superfix 0; the 2-covering itself is given by

$$m_1^0 = -d_{21}d_{31}, \quad m_2^0 = -d_{12}d_{32}, \quad m_3^0 = -d_{13}d_{23}.$$

We shall also need to know the 2-coverings corresponding to the 2-division points. That corresponding to $(c_1, 0)$, for example, is given by

$$m_1 = -a_0 a_1, \quad m_2 = d_{03} d_{21}, \quad m_3 = d_{02} d_{31}, \tag{55}$$

which can alternatively be written

$$m_1 = -a_0 a_1, \quad m_2 = -h/a_1 a_2, \quad m_3 = h/a_3 a_1.$$

It follows from the expressions for the $d_{ij}$ that, up to a squared factor, the discriminant of $d_{ij}$ is equal to $-a_i a_j$; thus in particular $d_{ij}$ has no repeated linear factor and it is a product of two linear factors over $k$ if and only if $-a_i a_j$ is in $k^{*2}$. If $i, j, k$ is a cyclic permutation of $1, 2, 3$ then

$$d_{0i}/d_{jk} = a_0 a_i/h = h/a_j a_k.$$

Moreover the resultant of $d_{ij}$ and $d_{ik}$ is $-4a_i^2 a_j a_k$, so that $d_{ij}$ and $d_{ik}$ cannot have a common root. The pencil (50) has six singular fibres, given by the roots of $d_{01} d_{02} d_{03} = 0$, and each singular fibre consists of four lines which form a skew quadrilateral. Thus each of the 48 lines on (51) is part of a singular fibre of one of the two pencils on $V$.

Martin Bright's thesis contains a dictionary which gives the Néron-Severi group of (51) over any field $k$. This group has rank at least 2 whenever (52) holds; subject to (52), it has rank greater than 2 if and only if up to fourth powers there is a relation of the form $a_j = 4a_i$ or $a_j = -a_i$ or $a_i a_j = a_k a_\ell$.

In order to apply Theorem 11.2, we must know when Condition D holds, and we must evaluate the relevent Legendre-Jacobi functions. This is where a splitting of cases becomes necessary. In what follows, we confine ourselves to the case when none of the $-a_i a_j$ is in $k^{*2}$, which is equivalent to requiring that all the $d_{ij}$ are irreducible over $k$.

**Lemma 12.1.** *Suppose that no $-a_i a_j$ is in $k^{*2}$. Then for any $\mathbf{m}$ which does not satisfy Condition D, one of $\mathbf{m}$ and $\mathbf{mm}^0$ can be chosen to be independent of $y$ and $z$. Moreover the group of such $\mathbf{m}$ has order exactly 8 (and consists of the inescapable part of the 2-Selmer group) if and only if $a_0 a_1 a_2 a_3$ is not a fourth power and no $a_i a_j$ is a square.*

What happens in the exceptional cases is as follows. If for example $a_2 a_3$ is a square then $(1, -a_1 a_2, -a_1 a_2)$ does not satisfy Condition D. Again, if $h$ is in $-k^{*2}$ then $(a_1 a_3, a_1 a_2, a_2 a_3)$ does not satisfy Condition D, whereas if $h$ is in $k^{*2}$ then $(a_1 a_2, a_2 a_3, a_3 a_1)$ does not satisfy Condition D. In each of these cases, the group of inescapable elements of the 2-Selmer group acquires one extra generator, which is the $\mathbf{m}$ just listed; and this provides a straightforward description of Condition E. If some $a_i a_j$ and one of $\pm h$ are both squares, then we acquire two extra generators in this way.

We can now state the main result of this subsection, which is simply the special-ization of Theorem 11.2 to our case, and which therefore requires no further proof. The set $\mathscr{S}$ of bad places consists of the infinite places, the primes which divide $2a_0a_1a_2a_3$ and a basis for the ideal class group of $k$. Denote by $\mathscr{A}$ the closure of the set of points $\alpha \times \beta$ in $\mathscr{N}^2$ at which (50) is locally soluble for $y = \alpha, z = \beta$ at each place of $\mathscr{S}$ and all the Legendre-Jacobi conditions associated with any pencil of conics (53) hold.

**Theorem 12.2.** *Suppose that (51) is everywhere locally soluble and such that $a_0a_1a_2a_3$ is a square, and that no $-a_ia_j$ is in $k^{*2}$. Assume Schinzel's Hypothesis and the finiteness of* $\text{III}$. *If $\mathscr{A}$ is not empty and Condition D holds, then (51) contains rational points.*

As was remarked at the end of Sect. 11, we can here replace Condition D by the weaker Condition E.

The solubility of the pencil of conics (53) is equivalent to three Legendre-Jacobi conditions, of which a typical one is

$$L(\mathscr{B}; -d_{i\ell}d_{j\ell}, d_{k\ell}) = 1. \tag{56}$$

There are 12 conditions of this kind, but they are not all independent. Indeed in the notation of Lemma 8.3 the continuous conditions, which form a subgroup there called $\Lambda_0$, are all Brauer-Manin; and Bright's table shows that in the most general case satisfying (52) there is only one algebraic Brauer-Manin condition. In general the twelve conditions of the form (56) all reduce to $F_{12}F_{23}F_{31} = 1$ where

$$F_{ij} = L(\mathscr{B}; -d_{i\ell}d_{j\ell}, d_{k\ell}; \alpha, \beta) = L(\mathscr{B}; -d_{ik}d_{jk}, d_{\ell k}; \alpha, \beta).$$

If however one of the $a_ia_j$ is a square then the corresponding condition $F_{ij} = 1$ is also in $\Lambda_0$. The remarks which follow Lemma 12.1 show that Condition D cannot then hold, but Condition E may still hold in some part of $\mathscr{A}$. One can evaluate the $F_{ij}$ by using the formulae which follow (24). Of the surfaces (51) defined over $\mathbf{Q}$ which satisfy (52) and have the $a_i$ integral with each $|a_i| < 16$, there are just two which are everywhere locally soluble but do not have a solution in $\mathbf{Q}$. They are

$$2X_0^4 + 9X_1^4 = 6X_2^4 + 12X_3^4 \quad \text{and} \quad 4X_0^4 + 9X_1^4 = 8X_2^4 + 8X_3^4.$$

The first of these fails the condition $F_{12}F_{23}F_{31} = 1$ and the second has $a_0a_1$ square and fails the condition $F_{01} = 1$.

Using the methods of Cassels [58] we can carry out a second descent on some of the surfaces considered in this subsection, and thereby prove that certain equations (51) are insoluble or do not admit weak approximation. The prettiest result that has been obtained in this way is as follows.

**Lemma 12.3.** *Suppose that $X_0^4 + 4X_1^4 = W_0^2 - 2W_1^2$ for $X_0, X_1, W_0, W_1$ in $\mathbf{Z}$ such that no prime $p \equiv 7 \mod 8$ divides both $W_0$ and $W_1$. Then $|W_0| \not\equiv 5$ or $7 \mod 8$.*

This is a weak approximation property, but of a rather unusual sort; and it appears unlikely that it corresponds to a Brauer-Manin condition.

## 12.2 Some Kummer Surfaces

In this subsection we consider Kummer surfaces of the form

$$Z^2 = f^{(1)}(X)f^{(2)}(Y) \tag{57}$$

defined over an algebraic number field $k$, where the $f^{(i)}$ are separable quartic polynomials. For (57) to be everywhere locally soluble, for each place $v$ of $k$ there must exist $c_v$ in $k_v^*$ such that both the equations

$$U^2 = c_v f^{(1)}(X) \text{ and } V^2 = c_v f^{(2)}(Y)$$

are soluble in $k_v$. For (57) to be soluble in $k$ requires the stronger condition that there exists $c$ in $k^*$ such that both the equations

$$U^2 = c f^{(1)}(X) \text{ and } V^2 = c f^{(2)}(Y) \tag{58}$$

are everywhere locally soluble. For the existence of the $c_v$ to imply the existence of $c$ is a local-to-global theorem, and the obstruction to this turns out to be a Brauer-Manin obstruction. In my view, this is the most interesting feature of the whole argument.

To be able to use the methods of Sect. 11 on the pair of equations (58), we must require that their Jacobians each have all their 2-division points rational. In this case it turns out that the Brauer-Manin obstruction introduced in the previous paragraph is trivial; in other words, we can always find the $c$ that we need. Call one such value $c^0$; then we can replace $c^0$ by any $c$ which is close to $c^0$ at all the bad places of (57) and is such that the good primes $\mathfrak{p}$ which divide it to an odd power are such that both equations (58) are soluble in $k_\mathfrak{p}$. To prove solubility of (57) we introduce well-chosen primes into $c$ in such a way as to reduce the orders of the 2-Selmer groups of both the underlying Jacobians to 8. This requires some intricate but elementary arguments; and for these we need to assume that for each Jacobian there are two primes which are bad in a specified way for that curve but which are good for the other. Full details can be found in [23], but this is definitely not recommended reading.

## 12.3 Diagonal Cubic Surfaces

In this subsection we consider diagonal cubic surfaces

$$a_0 X_0^3 + a_1 X_1^3 = a_2 X_2^3 + a_3 X_3^3 \tag{59}$$

over certain algebraic number fields $k$. Without loss of generality we can assume that the $a_i$ in (59) are integers. To show that (59) has a rational solution it is enough to show that there exists $c$ in $k^*$ such that each of the two curves

$$a_0 X_0^3 + a_1 X_1^3 = cX^3, \quad \text{and} \quad a_2 X_2^3 + a_3 X_3^3 = cX^3 \tag{60}$$

is soluble. The hypothesis that (59) is everywhere locally soluble implies that for each place $v$ in $k$ there exists $c_v$ in $k_v^*$ such that each of

$$a_0 X_0^3 + a_1 X_1^3 = c_v X^3, \quad \text{and} \quad a_2 X_2^3 + a_3 X_3^3 = c_v X^3$$

is soluble in $k_v$. The first step in the argument is to deduce from the existence of the $c_v$ the existence of $c$ in $k^*$ such that each of the two equations (60) is everywhere locally soluble. In contrast with what happened in the previous subsection, such a $c$ always exists; and indeed if $\mathscr{S}$ is any given finite set of places of $k$, we can choose $c$ integral and such that $c/c_v$ is in $k_v^{*3}$ for each $v$ in $\mathscr{S}$. Following the methods of Sect. 11, we denote by $\mathbf{L}^1$ the affine line with the origin deleted. Let $\mathscr{S}$ be a set of bad places for the surface (59), which means that $\mathscr{S}$ must contain all the primes of $k$ dividing $3a_0a_1a_2a_3$ and a basis for the ideal class group of $k$; and let $\mathscr{B} \supset \mathscr{S}$ be a set of bad places for the pair of curves (60), so that $\mathscr{B}$ must also contain all the primes dividing $c$. Under the topology induced by $\mathscr{S}$, let $\mathscr{A}$ be the open subset of $\mathbf{L}^1(k)$ on which each of the two curves (60) is locally soluble at each place of $\mathscr{S}$, let $c_0$ be a given point of $\mathscr{A}$ and let $\mathscr{N}_0 \subset \mathscr{A}$ be an open neighbourhood of $c_0$. Because of the possible presence of Brauer-Manin obstructions, it is not necessarily true that there exists $c$ in $\mathscr{N}_0$ such that the two equations (60) are both soluble. But one may still ask what additional assumptions are needed in order to prove solubility by the methods of Sect. 11 – always of course on the basis that $\mathrm{III}$ is finite.

The Jacobians of the two curves (60) are

$$Y_0^3 + Y_1^3 = a_0 a_1 c Y^3 \quad \text{and} \quad Y_2^3 + Y_3^3 = a_2 a_3 c Y^3 \tag{61}$$

respectively. The obvious descent to apply to each of them is the $\rho$-descent, where $\rho = \sqrt{-3}$. Applying this to the elliptic curve

$$X^3 + Y^3 = AZ^3 \tag{62}$$

replaces it by the equations

$$\rho X + \rho^2 Y = m_1 Z_1^3, \quad \rho^2 X + \rho Y = m_2 Z_2^3, \quad X + Y = AZ_3^3 / m_1 m_2$$

where $Z = Z_1 Z_2 Z_3$. Here $m_1, m_2, Z_1, Z_2$ are in $K = k(\rho)$ and if $\rho$ is not in $k$ then $m_1, m_2$ are conjugate over $k$, as are $Z_1, Z_2$; but $Z_3$ is in $k$. It would appear natural to work in $K$ rather than $k$, since if (59) is soluble in $K$ it is soluble in $k$. But actually

our methods could not then be applied, for complex multiplication by $\rho$ induces an isomorphism on (62), so that the Mordell-Weil group of (62) over $K$ has an even number of generators of infinite order and there is no possibility of applying Lemma 4.6. Thus a prerequisite for applying the methods of Sect. 11 is the unexpected constraint:

$$\sqrt{-3} \text{ is not in } k. \tag{63}$$

This does however allow us to take $k = \mathbf{Q}$, for example. But even if (63) holds, there is considerable interplay between the descent theory over $K$ and that over $k$; and it seems necessary to make use of this interplay in the argument.

The basic idea is to write $c$ as a product of primes in $\mathscr{S}$ (which are forced on us by the choice of $\mathscr{N}_0$) and some other well-chosen primes; the latter make up the set $\mathscr{B} \setminus \mathscr{S}$. We need to choose the latter so that the $\rho$-Selmer group of each of the curves (61) has order 9; and following the precedent of Sect. 11 we expect to do this by adjoining additional primes one by one to $\mathscr{B}$, always preserving the local solubility of the curves (60) and keeping $c$ within $\mathscr{N}_0$. The latter condition simply means that each new prime $\mathfrak{p}$ should be close to 1 in our topology and should be such that $a_0/a_1$ and $a_2/a_3$ are in $k_\mathfrak{p}^{*3}$. But here we encounter the final pair of complications. To adjoin one more prime divides or multiplies the order of each $\rho$-Selmer group by 3. If one of these orders has already been reduced to 9 we cannot reduce it further; so adjoining one more prime can no longer improve the situation. Instead we eventually reach the stage when we have to adjoin two more primes simultaneously, in such a way that the order of one of the $\rho$-Selmer groups remains unchanged, while the order of the other is divided by 9. To be able to reduce the orders of both $\rho$-Selmer groups to 9, we therefore need the initial choice of $c$ to satisfy the following additional condition:

> The product of the orders of the $\rho$-Selmer groups of the two curves (61) is a power of 9.

As should be clear from the preceding discussion, the truth or falsehood of this statement depends only on $\mathscr{N}_0$ (provided it is small enough) and not on the value of $c$ within $\mathscr{N}_0$. In other words, it depends only on the choice of $c_0$; and we need to show that we can choose $c_0$ so that (in addition to the previous requirements) this condition holds at $c_0$. Having done all this, we still need the equivalent of Condition D or Condition E.

However, at the end of all these complications we do obtain Theorem 12.4 below; the full details of the proof can be found in [18]. The sufficient conditions stated in Theorem 12.4 are clumsy and could certainly be improved; but I do not believe that this method is powerful enough to replace them by the Brauer-Manin conditions.

**Theorem 12.4.** *Let $k$ be an algebraic number field not containing the primitive cube roots of unity. Assume that $\text{Ш}$ is always finite. If (59) is everywhere locally soluble and the $a_i$ are all cubefree, then each of the following criteria is sufficient for the solubility of (59) in $k$.*

(i) *There exist primes $\mathfrak{p}_1, \mathfrak{p}_3$ of $k$ not dividing 3 such that $a_1$ is a non-unit at $\mathfrak{p}_1$ and $a_3$ is a non-unit at $\mathfrak{p}_3$, but for $j = 1$ or 3 the three $a_i$ with $i \neq j$ are units at $\mathfrak{p}_j$.*

(ii) *There is a prime $\mathfrak{p}$ of $k$ not dividing $3$ such that $a_1$ is a non-unit at $\mathfrak{p}$ but the other $a_i$ are units there; and $a_2, a_3, a_4$ are not all in the same coset of $k_{\mathfrak{p}}^{*3}$.*

(iii) *There is a prime $\mathfrak{p}$ of $k$ not dividing $3$ such that exactly two of the $a_i$ are units at $\mathfrak{p}$, and (59) is not birationally equivalent to a plane over $k_{\mathfrak{p}}$.*

## 13   The Case of One Rational $2$-Division Point

It is possible to carry out a 2-descent without using information about a field extension provided that the elliptic curve involved has one rational 2-division point – though it is then necessary to implement the process in two stages. The details of this process have been worked out, with increasing degrees of sophistication, in [15, 59] and Chap. II of [14]. I sketch it in this section.

We are concerned with pencils of 2-coverings whose pencil of Jacobians has the form

$$Y^2 = (X - c(U,V))(X^2 - d(U,V))$$

where $c, d$ are homogeneous polynomials in $k[U,V]$ with $\deg d = 2 \deg c$. We start by recalling the standard machinery for 2-descent on

$$E' : Y^2 = (X - c)(X^2 - d)$$

for $c, d$ in $k$ and $d$ not in $k^2$.

If $O'$ is the point at infinity on $E'$ and $P'$ the 2-division point $(c, 0)$ then there is an isogeny $\phi' : E' \to E'' = E'/\{O', P'\}$ where $E''$ is

$$E'' : Y_1^2 = (X_1 + 2c)(X_1^2 + 4(d - c^2));$$

the places of bad reduction for $E''$ are the same as those for $E'$. Explicitly, $\phi'$ is given by

$$X_1 = \frac{d - X^2}{c - X} - 2c, \quad Y_1 = \frac{Y(X^2 - 2cX + d)}{(X - c)^2}.$$

There is also a dual isogeny $\phi'' : E'' \to E'$, and $\phi'' \circ \phi'$ and $\phi' \circ \phi''$ are the doubling maps on $E'$ and $E''$ respectively. We are primarily interested in the case when neither $d$ nor $c^2 - d$ is a square in $k$, so that $E'$ and $E''$ each contain only one primitive 2-division point defined over $k$.

The elements of $\mathrm{H}^1(k, \{O', P'\}) \sim k^*/k^{*2}$ classify the $\phi'$-coverings of $E''$; the covering corresponding to the class of $m'$ is

$$V_1^2 = m'(X_1 + 2c), \quad V_2^2 = m'(X_1^2 + 4(d - c^2)) \tag{64}$$

with the obvious two-to-one map to $E''$. The $\phi'$-covering corresponding to $P''$ is given by $m' = d$. Similarly the $\phi''$-coverings of $E'$ are classified by the elements of $\mathrm{H}^1(k, \{O'', P''\}) \sim k^*/k^{*2}$, the covering corresponding to the class of $m''$ being

$$W_1^2 = m''(X - c), \quad W_2^2 = m''(X^2 - d). \tag{65}$$

The $\phi''$-covering corresponding to $P'$ is given by $m'' = c^2 - d$. We denote by $S_2'$ the 2-Selmer group of $E'$, and by $S_\phi'$, $S_\phi''$ the $\phi'$-Selmer group of $E''$ and the $\phi''$-Selmer group of $E'$ respectively.

Write $K = k(d^{1/2})$; then the group of 2-coverings of $E'$ is naturally isomorphic to $K^*/K^{*2}$, where the 2-covering corresponding to the class of $a + bd^{1/2}$ is given by

$$Z_1^2 = (a^2 - db^2)(X - c), \quad (Z_2 \pm d^{1/2}Z_3)^2 = (a \pm bd^{1/2})(X \pm d^{1/2}).$$

In homogeneous form, this can be written

$$\left.\begin{array}{l} Z_2^2 + dZ_3^2 = aZ_1^2/(a^2 - db^2) + (ac + bd)Z_0^2, \\ 2Z_2Z_3 = bZ_1^2/(a^2 - db^2) + (a + bc)Z_0^2. \end{array}\right\} \tag{66}$$

Call this curve $\Gamma'$; then the map $\Gamma' \to E'$ has degree 4 and is given by

$$X = \frac{Z_1^2}{(a^2 - db^2)Z_0^2} + c, \quad Y = \frac{Z_1(Z_2^2 - dZ_3^2)}{(a^2 - db^2)Z_0^3}.$$

The map $\Gamma' \to E'$ can be factorized as $\Gamma' \to C'' \to E'$, where $C''$ is the $\phi''$-covering of $E'$ given by (65) with $m'' = a^2 - db^2$ and the map $\Gamma' \to C''$ is

$$W_1 = Z_1/Z_0, \quad W_2 = (Z_2^2 - dZ_3^2)/Z_0^2.$$

Conversely, suppose that we have a curve of genus 1 defined over $k$ and given by the equations

$$\left.\begin{array}{l} \alpha_0 U_0^2 + \alpha_1 U_1^2 + \alpha_2 U_2^2 + \alpha_3 U_3^2 + 2\alpha_4 U_2 U_3 = 0, \\ \beta_0 U_0^2 + \beta_1 U_1^2 + \beta_2 U_2^2 + \beta_3 U_3^2 + 2\beta_4 U_2 U_3 = 0, \end{array}\right\} \tag{67}$$

where the $\alpha_i, \beta_i$ are in $\mathfrak{o}$. We have just seen that any 2-covering of an elliptic curve with one rational 2-division point can be put in this form, and we shall now prove the converse. Write $d_{ij} = \alpha_i\beta_j - \alpha_j\beta_i$; then the curve (67) takes the more convenient form

$$\left.\begin{array}{l} d_{10}U_0^2 + d_{12}U_2^2 + 2d_{14}U_2U_3 + d_{13}U_3^2 = 0, \\ d_{01}U_1^2 + d_{02}U_2^2 + 2d_{04}U_2U_3 + d_{03}U_3^2 = 0. \end{array}\right\} \tag{68}$$

If we write $U_0 = 2Z_0(d_{14}^2 - d_{12}d_{13})$ and $U_1 = Z_1/4d_{34}(d_{14}^2 - d_{12}d_{13})$, this last pair of equations can be identified with (66) provided that

$$a = -2(2d_{14}d_{34} + d_{13}d_{23})(d_{14}^2 - d_{12}d_{13}), \quad b = d_{01}^{-1}d_{13}(d_{14}^2 - d_{12}d_{13}),$$
$$c = 4d_{04}d_{14} - 2d_{02}d_{13} - 2d_{03}d_{12}, \quad d = 4d_{01}^2(d_{23}^2 + 4d_{24}d_{34});$$

it also follows from these that

$$c^2 - d = 16(d_{04}^2 - d_{02}d_{03})(d_{14}^2 - d_{12}d_{13}),$$
$$m'' = a^2 - db^2 = 16d_{34}^2(d_{14}^2 - d_{12}d_{13})^3.$$

We assume that $d(c^2 - d) \neq 0$, so that (67) defines a nonsingular curve of genus 1.

Now let $\mathscr{S}$ be a finite set of places which contains the infinite places, the primes which divide 2, the odd primes of bad reduction for $E'$ (or $E''$) and a set of generators for the ideal class group of $k$. For any $v$ in $\mathscr{S}$ we write

$$V_v' = \mathrm{H}^1(k_v, \{O', P'\}) \sim k_v^*/k_v^{*2}$$

and similarly for $V_v''$; and we denote by $W_v'$ the image of $E''(k_v)/\phi'E'(k_v)$ in $V_v'$ and similarly for $W_v''$. Thus $m'$ lies in $W_v'$ if and only if $\Gamma'$ is soluble over $k_v$, and similarly for $W_v''$. There is a non-degenerate canonical pairing

$$V_v' \times V_v'' \to \{\pm 1\} \tag{69}$$

induced by the Hilbert symbol, under which the orthogonal complement of $W_v'$ is $W_v''$. As in Sect. 10, we write

$$V_{\mathscr{S}}' = \oplus_{v \in \mathscr{S}} V_v', \quad W_{\mathscr{S}}' = \oplus_{v \in \mathscr{S}} W_v'$$

and similarly for $V''$ and $W''$. The machinery in the first half of Sect. 10 needs to be modified to take account of the changed circumstances, but the proofs involve no new ideas.

**Lemma 13.1.** *Let $\mathscr{S}_0$ consist of the infinite places, the even primes, and a set of generators for the ideal class group of $k$. For each $v$ in $\mathscr{S}$ there exist subspaces $K_v' \subset V_v'$ and $K_v'' \subset V_v''$ such that*

(i) *$K_v''$ is the orthogonal complement of $K_v'$ under the pairing (69);*
(ii) *$V_{\mathscr{S}}' = U_{\mathscr{S}}' \oplus K_{\mathscr{S}}'$ and $V_{\mathscr{S}}'' = U_{\mathscr{S}}'' \oplus K_{\mathscr{S}}''$ where $U_{\mathscr{S}}', U_{\mathscr{S}}''$ are the images of $X_{\mathscr{S}} \times X_{\mathscr{S}} = (\mathfrak{o}_{\mathscr{S}}^*/\mathfrak{o}_{\mathscr{S}}^{*2})^2$ in $V_{\mathscr{S}}'$ and $V_{\mathscr{S}}''$ respectively;*
(iii) *If $v$ is not in $\mathscr{S}_0$ we can take $K_v'$ and $K_v''$ to be the images of $(\mathfrak{o}_v^*/\mathfrak{o}_v^{*2})^2$.*

It follows from (69) that there is a non-degenerate canonical pairing

$$V_{\mathscr{S}}' \times V_{\mathscr{S}}'' \to \{\pm 1\} \tag{70}$$

and from (i) that $K_{\mathscr{S}}'' = \oplus_{v \in \mathscr{S}} K_v''$ is the orthogonal complement of $K_{\mathscr{S}}'$ under this pairing.

**Lemma 13.2.** *If $\mathscr{S} \supset \mathscr{S}_0$ then $S_\phi'$ is isomorphic to each of $U_{\mathscr{S}}' \cap W_{\mathscr{S}}'$, the left kernel of the map $U_{\mathscr{S}}' \times W_{\mathscr{S}}'' \to \{\pm 1\}$ induced by (70), and the left kernel of the map $W_{\mathscr{S}}' \times U_{\mathscr{S}}'' \to \{\pm 1\}$ induced by (70). A similar result holds for $S_\phi''$.*

Let $t_{\mathscr{S}}' : V_{\mathscr{S}}' \to U_{\mathscr{S}}'$ be the projection along $K_{\mathscr{S}}'$ and similarly for $t_{\mathscr{S}}''$. We now diverge from the notation of Sect. 10, writing

$$\mathbf{U}'_{\mathscr{S}} = U'_{\mathscr{S}} \cap (W'_{\mathscr{S}} + K'_{\mathscr{S}}), \quad \mathbf{W}'_{\mathscr{S}} = W'_{\mathscr{S}}/(W'_{\mathscr{S}} \cap K'_{\mathscr{S}})$$

and similarly for $\mathbf{U}''_{\mathscr{S}}$ and $\mathbf{W}''_{\mathscr{S}}$; as in Sect. 10, the map $t'_{\mathscr{S}}$ induces an isomorphism $\tau'_{\mathscr{S}} : \mathbf{W}'_{\mathscr{S}} \to \mathbf{U}'_{\mathscr{S}}$, and there is an analogous isomorphism $\tau''_{\mathscr{S}} : \mathbf{W}''_{\mathscr{S}} \to \mathbf{U}''_{\mathscr{S}}$. The pairing (70) induces pairings

$$\mathbf{U}'_{\mathscr{S}} \times \mathbf{W}''_{\mathscr{S}} \to \{\pm 1\}, \quad \mathbf{W}'_{\mathscr{S}} \times \mathbf{U}''_{\mathscr{S}} \to \{\pm 1\} \tag{71}$$

and the action of $\tau'_{\mathscr{S}} \times (\tau''_{\mathscr{S}})^{-1}$ takes the first pairing into the second. The left kernel of either of these pairings is isomorphic to $S'_\phi$ and the right kernel to $S''_\phi$. The action of $\tau'_{\mathscr{S}} \times 1$ takes the first pairing into the pairing

$$\mathbf{W}'_{\mathscr{S}} \times \mathbf{W}''_{\mathscr{S}} \to \{\pm 1\}.$$

Our objective is to prove the solubility in $k$ of pencils of curves (67) under suitable conditions. The appropriate modification of Lemma 11.1 is as follows.

**Lemma 13.3.** *Suppose that $P'$ is the only primitive 2-division point of $E'$ defined over $k$ and similarly for $P''$ on $E''$. If the orders of $S'_\phi$ and $S''_\phi$ are 2 and 4 respectively then the order of $S'_2$ is at most 4.*

*Proof.* Let $\Gamma'$ be a 2-covering of $E'$ and denote by $C''$ the quotient of $\Gamma'$ by the action of the group $\{O', P'\}$; then $C''$ is a $\phi''$-covering of $E'$ and we have a commutative diagram

$$
\begin{array}{ccccc}
E' & \xrightarrow{\phi'} & E'' & \xrightarrow{\phi''} & E' \\
\| & & \| & & \| \\
\Gamma' & \longrightarrow & C'' & \longrightarrow & E'
\end{array}
$$

where the first two vertical double lines mean that $\Gamma'$ and $C''$ are principal homogeneous spaces for $E'$ and $E''$ respectively. If $\Gamma'$ is identified with the element $f$ of $\mathrm{H}^1(k, E'[2])$ then $C''$ is identified with $\phi' \circ f$ as an element of $\mathrm{H}^1(k, E''[\phi''])$. If $\Gamma'$ is in $S'_2$ then $C''$ is in $S''_\phi$; so we can construct all the elements of $S'_2$ by lifting back the elements of $S''_\phi$. But by hypothesis $P''$ is not in $\phi'E'(k)$, so the two elements of $S'_\phi$ must correspond to the points $O''$ and $P''$ as members of $E''(k)/\phi'E'(k)$; hence regarded as elements of $S'_2$ they are equivalent. In other words, $E''$ regarded as an element of $S''_\phi$ lifts back to only one element of $S'_2$; so the same is true of each element of $S''_\phi$. $\qquad\square$

We now have to study simultaneously the $\phi'$-descent on $E''$ and the $\phi''$-descent on $E'$. As in Sect. 11, by introducing a sequence of well-chosen primes we reduce $S'_\phi$ and $S''_\phi$ until we can apply Lemma 13.3; but the process is more complicated than in Sect. 11. The strongest version of the argument is due to Wittenberg [14]; assuming Schinzel's Hypothesis and the finiteness of $\mathrm{III}$, to prove solubility he needs little more than the triviality of the Brauer-Manin obstruction.

# 14 Del Pezzo Surfaces of Degree 4

Let $V$ be a Del Pezzo surface of degree 4 (that is, the smooth intersection of two quadrics in $\mathbf{P}^4$) defined over an algebraic number field $k$. Salberger and Skorobogatov [60] have shown that the only obstruction to weak approximation on $V$ is the Brauer-Manin obstruction, and a more elementary proof can be found in [61].

**Theorem 14.1.** *Suppose that $V(k)$ is not empty. Let $\mathscr{A}$ be the subset of the adelic space $V(\mathbf{A})$ consisting of the points $\prod P_v$ such that*

$$\sum \mathrm{inv}_v(A(P_v)) = 0 \text{ in } \mathbf{Q}/\mathbf{Z}$$

*for all $A$ in the Brauer group $\mathrm{Br}(V)$. Then the image of $V(k)$ is dense in $\mathscr{A}$.*

The idea behind the proof in [61] is that we can use the existence of a point of $V(k)$ to fibre $V$ by conics. Theorem 9.4 now allows us to find a positive 0-cycle of degree 8 on $V$ defined over $k$ satisfying pre-assigned approximation conditions; and the proof is then completed by a modification of an argument of Coray [62]. Coray's result is Theorem 14.3 below; it will probably turn out to be a fundamental tool in the Diophantine theory of Del Pezzo equations of degree 4. Lemma 14.2 is weaker than Theorem 14.3, but appears to be a necessary step in the proof of the latter.

**Lemma 14.2.** *Let $V$ be a Del Pezzo surface of degree* 4*, defined over a field $L$ of characteristic* 0*. If $V$ contains a positive* 0*-cycle of degree* 2 *and a positive* 0*-cycle of odd degree $n$, both defined over $L$, then $V(L)$ is not empty.*

*Proof.* We can suppose $V$ embedded in $\mathbf{P}^4$ as the intersection of two quadrics. We proceed by induction on $n$. If the given 0-cycle of degree 2 consists of the two points $P'$ and $P''$ then we can suppose that they are conjugate over $L$ and distinct, because otherwise the lemma would be trivial. By a standard result, there are infinitely many points on $V$ defined over $L(P')$ and hence infinitely many positive 0-cycles of degree 2 defined over $L$. Choose $d$ so that

$$2d(d+1) > n > 2d(d-1)$$

and let $\{P'_i, P''_i\}$ be $\frac{1}{2}\{2d(d+1) - n - 1\}$ distinct pairs of points of $V$, the points of each pair being conjugate over $L$. The hypersurfaces of degree $d$ cut out on $V$ a system of curves of dimension $2d(d+1)$; hence there is at least a pencil of such curves passing through the $P'_i$ and $P''_i$ and the points of the given 0-cycle of degree $n$, and this pencil is defined over $L$. We have accounted for $2d(d+1) - 1$ of the $4d^2$ base points of the pencil; so the remaining ones form a positive 0-cycle of degree $2d(d-1) + 1$ defined over $L$. This completes the induction step unless $n = 2d(d-1) + 1$.

In this latter case we must have $d > 1$ because if $d = 1$ then $n = 1$ and the lemma is already proved; hence $2d(d+1) - n - 1 = 4d - 2 \geq 6$. Instead of the previous construction we now choose our pencil of curves to have double points at $P'_0$ and $P''_0$ and to pass through $\frac{1}{2}\{2d(d+1) - n - 7\}$ other pairs $P'_i, P''_i$ as well as through

the points of the given 0-cycle of degree $n$. In this case each of $P_0'$ and $P_0''$ is a base point of the pencil with multiplicity 4; so we have accounted for $2d(d+1)+1$ of the base points of the pencil, and the remaining ones form a positive 0-cycle of degree $2d(d-1)-1$ defined over $L$. This completes the induction step in this case.          □

**Theorem 14.3.** *Let $V$ be a del Pezzo surface of degree* 4, *defined over a field $L$ of characteristic* 0. *If $V$ contains a* 0-*cycle of odd degree defined over $L$ then $V(L)$ is not empty.*

*Proof.* By decomposing the 0-cycle into its irreducible components, we can assume that $V$ contains a positive 0-cycle $\mathfrak{a}$ of odd degree defined over $L$. We can write $V$ as the intersection of two quadrics, each defined over $L$; let $W$ be one of them. We can find a field $L_1 \supset L$ with $[L_1 : L] \leq 2$ and a point $P$ on $W$ defined over $L_1$. The lines on $W$ through $P$ are parametrised by the points of a conic, so we can find a field $L_2 \supset L_1$ with $[L_2 : L_1] \leq 2$ and a line $\ell$ on $W$, passing through $P$ and defined over $L_2$. The intersection of this line with another quadric containing $V$ cuts out on $V$ a positive 0-cycle of degree 2 defined over $L_2$. Applying Lemma 14.2 to $\mathfrak{a}$ and this 0-cycle, we obtain a point $P_2$ on $V$ defined over $L_2$. Repeating this argument for $\mathfrak{a}$ and the positive 0-cycle of degree 2 consisting of $P_2$ and its conjugate over $L_1$, we obtain a point $P_1$ on $V$ defined over $L_1$; and one further repetition of the argument gives us a point on $V$ defined over $L$.          □

To use and then collapse a field extension in this way is a device which probably has a number of uses. For such a collapse step to be feasible, the degree of the field extension needs to be prime to the degree of the variety; and this leads one to phrase the same property somewhat differently.

*Question 14.4.* Let $V$ be a variety defined over a field $K$, not necessarily of a number-theoretic kind. For what families of $V$ is it true that if $V$ contains a 0-cycle of degree 1 defined over $K$ then it contains a point defined over $K$?

As stated above, this is true for Del Pezzo surfaces of degree 4. For pencils of conics it is in general false, even for algebraic number fields $K$, as was shown at the end of Sect. 9. For Del Pezzo surfaces of degree 3 the question is open: I expect it to be true for algebraic number fields $K$ but false for general fields.

The methods of Sect. 13 have enabled Wittenberg [14] to prove the solubility of almost all Del Pezzo surfaces of degree 4 on which there is no Brauer-Manin obstruction. His starting point is as follows. Let $V$ be a nonsingular Del Pezzo surface of degree 4, defined over an algebraic number field $k$ and everywhere locally soluble. Then, after a field extension of odd degree, we can exhibit a family of hyperplane sections of $V$ which is of the form considered in Sect. 13. This family is parametrised by the points of $\mathbf{P}^3$ blown up along a certain curve and at four other points. The construction, which was first sketched in [15], is as follows.

The surface $V$ is the base locus of a pencil of quadrics; because $V$ is nonsingular, the pencil contains exactly 5 cones defined over $\bar{k}$ and these are all distinct. Hence one at least of them is defined over a field $k_1$ which is of odd degree over $k$; and by Theorem 14.3 it is enough to ask whether $V$ contains points defined over $k_1$. Henceforth we work over $k_1$. After a change of variables, we can assume that the

singular quadric just described has vertex $(1,0,0,0,0)$ and therefore an equation of the form $f(X_1,X_2,X_3,X_4) = 0$. By absorbing multiples of the other $X_i$ into $X_0$, we can write $V$ in the form

$$f(X_1,X_2,X_3,X_4) = 0, \quad aX_0^2 + g(X_1,X_2,X_3,X_4) = 0 \tag{72}$$

with $a \neq 0$. Now let $P$ be any point on $X_0 = 0$, let $Q$ be the quadric of the pencil (72) which passes through $P$, and let $\Pi$ be the tangent hyperplane to $Q$ at $P$. For general $P$ the curve of genus 1 in which $\Pi$ meets $V$ can be put in the form (68) and hence is of the type considered in Sect. 13. For provided that $P$ does not lie on $f = 0$, by a further change of variables we can take $P$ to be $(0,1,0,0,0)$ and require

$$f(X_1,X_2,X_3,X_4) = bX_1^2 + f_1(X_2,X_3,X_4).$$

The equation of $Q$ has no term in $X_1^2$, so by a further change of variables we can take it to have the form

$$aX_0^2 + cX_1X_4 + h(X_2,X_3,X_4) = 0 \tag{73}$$

with $c \neq 0$; this is equivalent to requiring the equation of $\Pi$ to be $X_4 = 0$. Since $V$ is given by $f = 0$ and (73), its intersection with $X_4 = 0$ has the required form.

This construction breaks down if $P$ lies on $V$ or is the vertex of one of the other singular quadrics of the pencil, because then $\Pi$ is no longer well-defined. To remedy this, what we do is to choose a point $P$ on $X_0 = 0$ together with a hyperplane $\Pi$ which touches at $P$ some quadric of the pencil (72). Thus $P$ should be considered as a point of the variety $W$ obtained by blowing up $X_0 = 0$ (which can be identified with $\mathbf{P}^3$) along the curve $V \cap \{X_0 = 0\}$ and at the vertices of the other four singular quadrics of the pencil.

Denote by $U$ the variety over $W$ whose fibres are the curves $V \cap \Pi$ in the construction above; then what we have obtained is a diagram

$$W \longleftarrow U \longrightarrow V$$

in which the left hand map is a fibration. The right hand map here is not a fibration, and it seems unlikely that there is even a subvariety of $U$ on which the restriction of the map is a fibration. But this is not important. What matters is the existence of a section – that is, a map $V \to U$ such that the composite map $V \to U \to V$ is the identity; and for this we only need the map $V \to U$ to be rational rather than everywhere defined. In the notation of (72) let $P_0 = (x_0,\ldots,x_4)$ be a point of $V$ with $x_0 \neq 0$, and choose $P = (0,x_1,x_2,x_3,x_4)$. The equation of $\Pi$ has no term in $X_0$; hence since $P$ lies on $\Pi$ so does $P_0$. This defines the rational map $V \to U$. Provided $V$ is everywhere locally soluble, so is $U$. If we can find a field extension $k_2/k_1$ of odd degree such that $U$ is soluble in $k_2$, then $V$ will also be soluble in $k_2$ and two applications of Theorem 14.3 will show that $V$ is soluble in $k$.

We cannot apply Wittenberg's results cited in Sect. 13 to $W$ directly, because $W$ is too big; but it is simple enough to find a line $L$ defined over $k_1$ in the $\mathbf{P}^3$ which underlies $W$ such that

- $L$ is in sufficiently general position, and
- The inverse image of $L$ in $U$ is everywhere locally soluble.

To do this, we choose any $P_1$ on $X_0 = 0$ and defined over $k_1$. The fibre above $P_1$ is locally soluble except at a finite set $\mathscr{S}$ of places. For each of these places there is a point of $U$ in the corresponding local field, and this maps down to a point of $\mathbf{P}^3$. Using weak approximation on $\mathbf{P}^3$ we can therefore find a point $P_2$ in $\mathbf{P}^3$ such that the fibre above $P_2$ is locally soluble at each place in $\mathscr{S}$. We can now take $L$ to be the line $P_1P_2$.

# References

1. Silverberg, A.: Open questions in arithmetic algebraic geometry. In: Arithmetic algebraic geometry, pp. 85–142. AMS, RI (2002)
2. Vaughan, R.C.: The Hardy-Littlewood method, 2nd edn. Cambridge (1997)
3. Davis, M., Matijasevič, Y., Robinson, J.: Hilbert's tenth problem: Diophantine equations: positive aspects of a negative solution. In: Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math. Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974), pp. 323–378. (loose erratum) Amer. Math. Soc., Providence, RI (1976)
4. Matiyasevich, Y.: Hilbert's tenth problem: what was done and what is to be done. In: Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Contemp. Math., vol. 270, pp. 1–47, Amer. Math. Soc., Providence, RI (2000)
5. Sir Swinnerton-Dyer P.: Weak approximation and $R$-equivalence on Cubic Surfaces. In: Peyre, E., Tschinkel, Y. (eds.) Rational points on algebraic varieties, Progress in Mathematics, vol. 199, pp. 357–404. Birkhäuser (2001)
6. Skorobogatov, A.N.: Beyond the Manin obstruction. Invent. Math. **135**, 399–424 (1999)
7. Harari, D.: Obstructions de Manin transcendantes. In: Number theory (Paris, 1993–1994). London Mathematical Society Lecture Note Series, vol. 235, pp. 75–87. Cambridge University Press, Cambridge (1996)
8. Bright, M., Sir Peter Swinnerton-Dyer: Computing the Brauer-Manin obstructions. Math. Proc. Camb. Phil. Soc. **137**, 1–16 (2004)
9. Manin, Yu.I.: Cubic forms. North-Holland, Amsterdam (1974)
10. Colliot-Thélène, J.-L., Sansuc, J.-J., Sir Peter Swinnerton-Dyer: Intersections of two quadrics and Châtelet surfaces. J. reine angew. Math. **373**, 37–107 (1987); **374**, 72–168 (1987)
11. Colliot-Thélène, J.-L., Sir Peter Swinnerton-Dyer: Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties. J. reine angew. Math. **453**, 49–112 (1994)
12. Sir Peter Swinnerton-Dyer: Rational points on pencils of conics and on pencils of quadrics. J. Lond. Math. Soc. **50**(2), 231–242 (1994)
13. Skorobogatov, A.: Torsors and rational points. Cambridge Tracts in Mathematics, vol. 144. Cambridge University Press, Cambridge (2001)
14. Wittenberg, O.: Intersections de deux quadriques et pinceaux de courbes de genre 1. Springer, Heidelberg (2007)
15. Bender, A.O., Sir Peter Swinnerton-Dyer: Solubility of certain pencils of curves of genus 1, and of the intersection of two quadrics in $\mathbf{P}^4$. Proc. Lond. Math. Soc. **83**(3), 299–329 (2001)

16. Colliot-Thélène, J.-L., Skorobogatov, A.N., Sir Peter Swinnerton-Dyer: Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points. Invent. Math. **134**, 579–650 (1998)

17. Sir Peter Swinnerton-Dyer: Arithmetic of diagonal quartic surfaces II. Proc. Lond. Math. Soc. **80**(3), 513–544 (2000)

18. Sir Peter Swinnerton-Dyer: The solubility of diagonal cubic surfaces. Ann. Scient. Éc. Norm. Sup. **34**(4), 891–912 (2001)

19. Kleiman, S.L.: Algebraic cycles and the Weil conjectures. In: Grothendieck, A., Kuiper, N.H. (eds.) Dix exposés sur la cohomologie des schémas, pp. 359–386. North-Holland, Amsterdam (1968)

20. Serre, J.-P.: Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). Séminaire Delange-Pisot-Poitou 1969/70, exp. 19

21. Borel, A.: Cohomologie de $SL_n$ et valeurs de fonctions zeta aux points entiers. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4), **4**(4), 613–636 (1977)

22. Tate, J.T.: On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. Sém. Bourbaki **306** (1966)

23. Swinnerton-Dyer, P.: The conjectures of Birch and Swinnerton-Dyer, and of Tate. In: Springer, T.A. (ed.) Proceedings of a Conference on Local Fields, Driebergen, 1966, pp. 132–157. Springer, NY (1967)

24. Rapaport, M., Schappacher, N., Schneider, P. (eds.): Beilinson's conjectures on special values of $L$-functions. Academic, NY (1988)

25. Hulsbergen, W.W.J.: Conjectures in arithmetic algebraic geometry. Vieweg, Braunschweig (1992)

26. Bloch, S.J.: Higher regulators, algebraic $K$-theory and zeta-functions of elliptic curves. CRM Monograph Series 11. AMS, RI (2000)

27. Bloch, S.J., Kato, K.: $L$-functions and Tamagawa numbers of motives. In: The Grothendieck Festschrift, vol. I, pp. 333–400. Birkhauser, Boston (1990)

28. Siegel, C.L.: Normen algebraischer Zahlen, Werke, Band IV, pp. 250–268

29. Raghavan, S.: Bounds for minimal solutions of Diophantine equations. Nachr. Akad. Wiss. Göttingen Math. -Phys. Kl. II, (9):109–114 (1975)

30. Faltings, G., Wüstholz, G.(eds.): Rational points, 3rd edn. Vieweg, Braunschweig (1992)

31. Mazur, B.: Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)

32. Merel, L.: Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent. Math. **124**, 437–449 (1996)

33. Rubin, K., Silverberg, A.: Ranks of elliptic curves. Bull. Amer. Math. Soc. **39**, 455–474 (2002)

34. Gebel, J., Zimmer, H.G.: Computing the Mordell-Weil group of an elliptic curve over $\mathbf{Q}$. In: Kisilevsky, H., Ram Murthy, M. (eds.) Elliptic curves and related topics. CRM Proceedings and Lecture Notes, vol. 4, pp. 61–83. AMS, RI (1994)

35. Gross, B., Kohnen, W., Zagier, D.: Heegner points and derivatives of $L$-series II. Math. Ann. **278**, 497–562 (1987)

36. Gross, B., Zagier, D.: Heegner points and derivatives of $L$-series. Invent. Math. **84**, 225–320 (1986)

37. Gross, B.: Kolyvagin's work for modular elliptic curves. In: Coates, J., Taylor, M.J. (eds.) L-functions and arithmetic, pp. 235–256. Cambridge (1991)

38. Kolyvagin, V.A.: Finiteness of $E(\mathbf{Q})$ and $\text{Ш}(E/\mathbf{Q})$ for a class of Weil curves. Izv. Akad. Nauk SSSR **52**, 522–540 (1988); translation in Math. USSR-Izv. **33**, 523–541 (1989)

39. Rubin, K.: Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. In: Viola, C. (ed.) Arithmetic theory of elliptic curves, pp. 167–234. Springer Lecture Notes 1716 (1999)

40. Beauville, A.: Complex algebraic surfaces, 2nd edn. London Mathematical Society Student Texts, 34, Cambridge University Press, Cambridge (1996)

41. Birch, B.J.: Homogeneous forms of odd degree in a large number of variables. Mathematika **4**, 102–105 (1957)

42. Hooley, C.: On nonary cubic forms. J. Reine Angew. Math. **386**, 32–98 (1988); **415**, 95–165 (1991); **456**, 53–63 (1994)
43. Browning, T.D.: An overview of Manin's conjecture for Del Pezzo surfaces. In: Duke, W., Tschinkel, Y. (eds.) Analytic number theory: A tribute to Gauss and Dirichlet. AMS, RI (2007)
44. Peyre, E.: Hauteurs et mesures de Tamagawa sur les variétés de Fano. Duke J. Math. **79**, 101–218 (1995)
45. Slater, J.B., Sir Peter Swinnerton-Dyer: Counting points on cubic surfaces I. Astérisque **251**, 1–11 (1998)
46. de la Brèteche, R., Browning, T.D.: On Manin's conjecture for singular Del Pezzo surfaces of degree four, I. Mich. Math. J (to appear)
47. de la Brèteche, R., Browning, T.D.: On Manin's conjecture for singular del Pezzo surfaces of degree four. II. Math. Proc. Cambridge Philos. Soc., **143**(3), 579–605 (2007)
48. de la Brèteche, R., Browning, T.D., Derenthal, U.: On Manin's conjecture for a certain singular cubic surface. Ann. Sci. École Norm. Sup. (4), **40**(1), 1–50 (2007)
49. de la Brèteche, R.: Sur le nombre de points de hauteur bornée d'une certaine surface cubique singulière. Astérisque **251**, 51–77 (1998)
50. de la Brèteche, R., Swinnerton-Dyer, P.: Fonction zêta des hauteurs associée à une certaine surface cubique. Bull. Soc. Math. France, **135**(1), (2007)
51. Swinnerton-Dyer, P.: A canonical height on $X_0^3 = X_1 X_2 X_3$. In: Diophantine geometry. CRM Series, vol. 4, pp. 309–322. Ed. Norm., Pisa (2007)
52. Colliot-Thélène, J.-L., Skorobogatov, A.N. Sir Peter Swinnerton-Dyer: Rational points and zero-cycles on fibred varieties: Schinzel's Hypothesis and Salberger's device. J. reine angew. Math. **495**, 1–28 (1998)
53. Sir Peter Swinnerton-Dyer: Some applications of Schinzel's hypothesis to diophantine equations. In: Györy, K., Iwaniec, H., Urbanowicz, J. (eds.) Number theory in progress, vol. 1, pp. 503–530. de Gruyter, Berlin (1999)
54. Milne, J.S.: Arithmetic duality theorems. Perspectives in Mathematics 1, Academic Press Inc., Boston (1986)
55. Skorobogatov, A.N., Swinnerton-Dyer, P.: 2-descent on elliptic curves and rational points on certain Kummer surfaces. Adv. Math. **198**, 448–483 (2005)
56. Colliot-Thélène, J.-L., Skorobogatov, A.N., Sir Peter Swinnerton-Dyer: Double fibres and double covers: paucity of rational points. Acta Arith. **79**, 113–135 (1997)
57. Bright, M.: Ph.D. dissertation. Cambridge (2002)
58. Cassels, J.W.S.: Second descents for elliptic curves. J. reine angew. Math. **494**, 101–127 (1998)
59. Colliot-Thélène, J.-L.: Hasse principle for pencils of curves of genus one whose Jacobians have a rational 2-division point (close variation on a paper of Bender and Swinnerton-Dyer). In: Rational points on algebraic varieties. Progr. Math. **199**, 117–161 (2001)
60. Salberger, P., Skorobogatov, A.N.: Weak approximation for surfaces defined by two quadratic forms. Duke J. Math. **63**, 517–536 (1991)
61. Swinnerton-Dyer, P.: Weak approximation on Del Pezzo surfaces of degree 4. In: Arithmetic of higher-dimensional algebraic varieties; Progr. Math. **226**, 235–257 (2004)
62. Coray, D.: Points algébriques sur les surfaces de Del Pezzo. C. R. Acad. Sci. Paris **284**, 1531–1534 (1977)