DIOPHANTINE EQUATIONS: PROGRESS AND PROBLEMS

1. *Introduction.*
A *Diophantine problem* over $\mathbf{Q}$ is concerned with the solutions either in $\mathbf{Q}$ or in $\mathbf{Z}$ of a finite system of polynomial equations

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

with coefficients in $\mathbf{Q}$. Without loss of generality we can obviously require the coefficients to be in $\mathbf{Z}$. 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 $\mathbf{Q}$. 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 $\mathbf{Z}$ or in $\mathbf{Q}$?

(B) For values of the c_j for which the system is soluble, is there an algorithm for exhibiting a solution?

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?

Most of these notes are concerned with (A) to (C), and after the Introduction (D) will not reappear until §8.

The attempts to answer these questions have led to the introduction of new ideas and these have generated new questions. On some of them I expect progress within the next decade, and I have restricted myself to these in the text below. Progress in mathematics usually means proven results; but there are cases where even 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 deep feeling for the structure of the subject have generally turned out to be a waste of time.) But I

have not included those problems (such as the Riemann Hypothesis and the Birch/Swinnerton-Dyer conjecture) on which I do not expect further progress within so short a timescale. The reader may also find it useful to read Silverberg [36], which has the same purpose as this article but rather little overlap with it.

Though the study of 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 they are actually very different and that 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 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 can also be applied to rational problems in projective space, because then the F_i in (1) are homogeneous and it does not matter whether we treat the variables X_ν as integral or rational. There is a brief discussion of this method in §8, and a comprehensive survey in [46].

Denote by V the variety defined by the equations (1) and let V' be any variety birationally equivalent to V over $\mathbf{Q}$. The problem of finding solutions of (1) in $\mathbf{Q}$ is the same as that of finding rational points on V, which is almost the same as that of finding rational points on V'. Hence (except possibly 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; and the way in which algebraic geometers classify varieties should provide at least a first rough guide to the classification of Diophantine problems — though they mainly study birational equivalence over $\mathbf{C}$ rather than over $\mathbf{Q}$. But it does at the moment seem that even for surfaces the geometric classification needs some refinements if it is to fit the number-theoretic results and conjectures.

Without loss of generality we can assume that V is absolutely irreducible. For if V has proper components defined over $\mathbf{Q}$ it is enough to ask the questions above for each of the proper components; and if V is the union of varieties conjugate over $\mathbf{Q}$ then any rational point on V lies on the intersection of these conjugates, which is a proper subvariety of V. Since we can desingularize V by a birational transformation defined over $\mathbf{Q}$, it is natural to concentrate on the case when V is projective and nonsingular.

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 essentially the same as 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 $\mathbf{Q}$.) 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 essential to consider these other fields also. If V is defined over a field K, the set of points on V defined over K will always be 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 $\mathbf{Q}$, for example, is that it is soluble in every $\mathbf{Q}_v$. The condition of solubility in every $\mathbf{Q}_v$ is computationally decidable; see §2. Moreover, at least for primes p for which the system (1) has good reduction mod p, the first step in deciding solubility in $\mathbf{Q}_p$ is to decide whether the reduced system is soluble in the finite field $\mathrm{GF}(p)$ of p elements.

Some geometers are already used to studying varieties over fields k which are not algebraically closed; what makes Diophantine problems special is the number-theoretic nature of the fields k. But it seems that only a few of the properties peculiar to such fields are useful in this context, so that a geometer need not learn much number-theory in order to work on Diophantine problems. On the other hand, a number-theorist would be wise to learn quite a lot of geometry.

Diophantine problems were first introduced by Diophantus of Alexandria, the last of the great Greek mathematicians, who lived at some time between 300 B.C. and 300 A.D.; but he was handicapped by having only one letter available to represent variables, all the others being used in classical Greek 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, by restricting to the special case when the equations are homogeneous. In those 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. Indeed he exhibited a polynomial $F(c; x_1, \ldots, x_n)$ such that there cannot exist an algorithm which will decide for every given 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 [10], pp 323-378 or [9]. The corresponding question for rational solutions is still open; I am among the very few who believe that it may have a positive answer.

But even if the answer to the analogue of Hilbert's tenth problem for rational solutions is positive, one must expect that a separate algorithm will be needed for each kind of variety. Thus we shall need not one algorithm but an infinity of them. So number theorists depend on the development by geometers of 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 number theorists have to concentrate on curves and surfaces, and on certain particularly simple kinds of variety in higher dimension.

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. 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 1 *Let W be an absolutely irreducible variety of dimension n defined over the finite field $k = \mathrm{GF}(q)$. Then $N(q)$, the number of points on W defined over k, satisfies*

$$|N(q) - q^n| < Cq^{n-1/2}$$

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 §3; but weaker results which are adequate for the present application were known much earlier. Since the singular points of W lie on a proper subvariety, there are at most $C_1 q^{n-1}$ of them, where C_1 is also computable. It follows that if q exceeds a computable bound depending only on the degree and dimension of W then W contains a nonsingular point defined over k.

Now let V be an absolutely irreducible variety defined over $\mathbf{Q}$. If V has good reduction at p, which happens for all but a finite computable set of primes p, denote that reduction by $\tilde{V}_p$. If p is large enough, it follows from the remarks above that $\tilde{V}_p$ contains a nonsingular point Q_p defined over $\mathrm{GF}(p)$. The result which follows, which is known as Hensel's Lemma though the idea of the proof goes back to Sir Isaac Newton, now shows that V contains a point P_p defined over $\mathbf{Q}_p$.

Lemma 2 *Let V be an absolutely irreducible variety defined over $\mathbf{Q}$ which has a well-defined reduction* mod p*, denoted by $\tilde{V}_p$. If $\tilde{V}_p$ contains a nonsingular point Q_p defined over* $\mathrm{GF}(p)$ *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 individually solubility in $\mathbf{R}$ and in finitely many $\mathbf{Q}_p$. Each of these checks can be shown to be a finite process, using ideas similar to those in the proof of Lemma 1.

A family $\mathcal{F}$ of varieties is said to satisfy the *Hasse Principle* if every V contained in $\mathcal{F}$ and defined over $\mathbf{Q}$ which satisfies the Hasse condition actually contains at least one point defined over $\mathbf{Q}$. Again, a family $\mathcal{F}$ is said to admit *weak approximation* if every V contained in $\mathcal{F}$ 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 $\mathcal{N}_v \subset V(\mathbf{Q}_v)$ open in the v-adic topology, there is a point P in $V(\mathbf{Q})$ which lies in each of the $\mathcal{N}_v$. In the special case when $\mathcal{F}$ 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 is in general not computable; for an important exception, see [43].

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. 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 1 *For a given family $\mathcal{F}$, 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 both more interesting and 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 *For a given V, or family $\mathcal{F}$, what can be said about the closure of $V(\mathbf{Q})$ in the adelic space $V(\mathbf{A})$?*

However, there are families for which Question 1 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 back up Question 1 with

Question 3 *For what kinds of families is either part of Question* 1 *a sensible question to ask?*

The only systematic obstruction to the Hasse Principle which is known is the Brauer-Manin obstruction, though obstructions can be found in the literature which are not Brauer-Manin. 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 $\imath_p : \mathrm{Br}(\mathbf{Q}_p) \simeq \mathbf{Q}/\mathbf{Z}$ for each p; and there is a canonical isomorphism $\imath_\infty : \mathrm{Br}(\mathbf{R}) \simeq \{0, \frac{1}{2}\}$, 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 $\imath_v$; 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 $\imath_p(A(P_p)) = 0$ for all p-adic points P_p on V. Thus 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

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

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. Even without any hypotheses on 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

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

Here only the abstract structure of $\mathrm{Br}(V)/\mathrm{Br}_1(V)$ is known; and in general there is no known way of finding Azumaya algebras which represent nontrivial elements of this quotient, though in a particular case Harari [20] 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 $\mathrm{Pic}(V \otimes \bar{\mathbf{Q}})$ is known. (For details of this, see [8].)

There is no known systematic way of determining $\mathrm{Pic}(V \otimes \bar{\mathbf{Q}})$ for arbitrary V, and there is strong reason to suppose that this is really a number-theoretic rather than a geometric problem. If V is defined over $\mathbf{Q}$ (rather than over an arbitrary algebraic number field) there is a tentative algorithm, depending on the Birch/Swinnerton-Dyer conjecture, for determining an algebraic number field K (depending on V) such that $\mathrm{Pic}(V \otimes \bar{\mathbf{Q}}) = \mathrm{Pic}(V \otimes K)$, and this may be the right first step towards determining $\mathrm{Pic}(V \otimes \bar{\mathbf{Q}})$; but one hopes not, because even for so elementary a variety as a cubic surface we may need to have $[K : \mathbf{Q}] \geq 51840$. It seems to me likely that a better approach to this question will be through the Tate conjectures, for which see §3; but this is a very long-term prospect. However, it is usually possible to determine $\mathrm{Pic}(V \otimes \bar{\mathbf{Q}})$ for any particular V that one is interested in.

Question 4 *Is there a general algorithm (even conjectural) for determining* $\mathrm{Pic}(V \otimes \bar{\mathbf{Q}})$ *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 $\mathcal{S}$ of proper subvarieties of V such that every point of $V(K)$ lies in $\mathcal{S}$. (Faltings' theorem, for which see §4, is the special case of this for curves.) This raises another question, similar to Question 4 but probably easier:

Question 5 *Is there an algorithm for determining* $\mathrm{Pic}(V)$ *where* V *is a variety defined over an algebraic number field?*

The Brauer-Manin obstruction was introduced by Manin [26] in order to bring within a single framework various sporadic counterexamples to the Hasse principle for rational surfaces. The theory of this obstruction has been extensively developed by Colliot-Thélène and Sansuc. In particular, for rational varieties they showed how to go back and forth between the Brauer-Manin condition and the descent condition for torsors under tori. They also 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 [12] and,

subject to Schinzel's hypothesis, [41] and [14].) It is generally believed 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 ([37], and see also [38]) has exhibited an obstruction to the Hasse principle on a bielliptic surface which is definitely not Brauer-Manin.

Question 6 *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 7 *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, and may even be equal to, all rationally connected varieties.

There are families $\mathcal{F}$ 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; but there are also alternative strategies. Implementing these falls naturally into two parts:

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

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

Both these strategies have been applied to pencils of conics, in each case assuming Schinzel's Hypothesis; the curious reader may wish to compare the approaches in [41] and in [14]. Except for Skorobogatov's example above, I know of no families for which it has been possible to carry out (i) but not (ii). 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 Condition D in [13], [42], [2] and [44]. However, in these cases it is not obvious that a condition stronger than the Brauer-Manin condition is actually necessary; and I am provisionally inclined to attribute the gap to clumsiness in the proofs.

Question 8 *When the Brauer-Manin condition is trivial, how can one make use of this fact?*

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 $k =$GF(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 GF(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 α_{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 ith cohomology group of W and the α_{ij} are the characteristic roots of the map induced by $\phi(q)$ on the ith cohomology. For each i duality implies that $B_i = B_{2d-i}$ and the $\alpha_{2d-i,j}$ are a permutation of the q^d/α_{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 [24].) 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 ith 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 $q = \mathrm{Norm}_{K/\mathbf{Q}}\mathfrak{p}$. The rules for forming the factors at the primes of bad reduction and at the infinite places can be found in [34]. 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 carries with it certain implications:

- $F(s)$ must be the product of a Dirichlet series and possibly some Gamma-functions, and the half-plane of absolute convergence for the Dirichlet series must have the form $\Re s > \sigma_0$ with $2\sigma_0$ in $\mathbf{Z}$.
- The Dirichlet series must be expressible as an Euler product $\prod_p f_p(p^{-s})$ where the f_p are rational functions.
- $F(s)$ must have an analytic continuation to the entire s-plane as a meromorphic function all of whose poles are in $\mathbf{Z}$.
- There must be a functional equation relating $F(s)$ and $F(2\sigma_0 - 1 - s)$.
- The zeroes of $F(s)$ in the critical strip $\sigma_0 - 1 < \Re s < \sigma_0$ must 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 9 *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 [6] which relate the behaviour of $\zeta_K(s)$ near $s = 1-m$ for integers $m > 1$ to the K-groups of $\mathfrak{O}_K$. I would be reluctant to claim that the L-series of a variety V contains all the information which one would like to have about the number-theoretical properties of V; but 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.

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 and 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 $L_1(s, V)$ must 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 remarks motivate the weak forms of the Birch/Swinnerton-Dyer conjecture (for which see §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 [45] or [40].

Question 10 *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 $L_i(s, V)$ about integer values of s; in them the leading coefficients are treated as elements of $\mathbf{C}^*/\mathbf{Q}^*$. (For a full account see [30] or [23].) Bloch and Kato ([4] and [5]) 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. 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 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 Γ of genus 0 has degree -2; hence by the Riemann-Roch theorem Γ 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 1 *Let a_0, a_1, a_2 be nonzero elements of* $\mathbf{Z}$. *If the equation*

$$a_0X_0^2 + a_1X_1^2 + a_2X_2^2 = 0$$

is soluble in $\mathbf{Z}$, *then it has a solution for which each $a_iX_i^2$ is absolutely bounded by $|a_0a_1a_2|$.*

Siegel [35] has given an answer to Question (B) over arbitrary algebraic number fields, and Raghavan [2] has generalized Siegel's work to quadratic forms in more variables.

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

If Γ 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 [15].

Question 11 *Is there an algorithm for computing $\Gamma(K)$ when Γ is a curve of general type defined over an algebraic number field K?*

The study of rational points on elliptic curves is now a major industry, almost entirely separate from the study of other Diophantine problems. If Γ 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; Weil's contribution was to extend this result to all Abelian varieties. Thanks to Mazur (see [27]) and Merel [47] 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 $\Gamma(K)$ can be embedded into a certain group which is finitely generated and computable. The process involved, which is known as the method of infinite descent, goes back to Fermat; for use in §6 I shall illustrate it below in a particularly simple case. By means of this process one can always compute an upper bound for the rank of the Mordell-Weil group of any particular Γ, 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 [32].

I now turn to the situation in which Γ is a curve of genus 1 defined over K but not necessarily containing a point defined over K. Let J be the Jacobian of Γ, defined as a curve whose points are in one-one correspondence with the divisors of degree 0 on Γ 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 Γ 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 Γ 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.

Suppose in particular that the elliptic curve J is defined over $\mathbf{Q}$ and has the form

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

where the distinguished point is taken to be the point at infinity. The three points $(c_i, 0)$ on J have order 2; they are called the 2-*division points*. To any rational point (x, y) on Γ there exist m_1, m_2, m_3 and y_1, y_2, y_3 such that

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

here the m_i are really elements of $\mathbf{Q}^*/\mathbf{Q}^{*2}$ but it is convenient to treat them as square-free integers. We must have $m_1 m_2 m_3 = m^2$ for some integer m, and after adjusting signs $my = y_1 y_2 y_3$. Conversely the equations

$$Y_i^2 = m_i(X - c_i) \ \ (i = 1, 2, 3) \quad \text{and} \quad mY = Y_1 Y_2 Y_3$$

for any m, m_i with $m_1 m_2 m_3 = m^2$ define a curve $\mathcal{C} = \mathcal{C}(m_1, m_2, m_3)$ and a four-to-one map $\mathcal{C} \to J$. If $\mathcal{C}(\mathbf{Q})$ is not empty, its image under this map is a coset of $2J(\mathbf{Q})$ in $J(\mathbf{Q})$, and we obtain all such cosets in this way. Thus we could find $J(\mathbf{Q})$ if we could decide which $\mathcal{C}$ are soluble in $\mathbf{Q}$.

After a change of variables we can assume that the c_i are in $\mathbf{Z}$. Define the *good primes* for J as those which do not divide $2(c_1 - c_2)(c_2 - c_3)(c_3 - c_1)$; then it is not hard to show that $\mathcal{C}$ is locally soluble at all good primes if and only if all the m_i are units at all good primes. So there are only finitely many $\mathcal{C}$ whose solubility in $\mathbf{Q}$ is at all hard to decide.

The curves $\mathcal{C}$ obtained in this way are called 2-*coverings* of J, and the process of obtaining them is called a 2-*descent*. They form a group under multiplication of the corresponding triples (m_1, m_2, m_3). The finite subgroup consisting of those 2-coverings which are everywhere locally soluble is called the 2-*Selmer group*. It is easily computable; and since there is a canonical embedding of $J(\mathbf{Q})/2J(\mathbf{Q})$ into the 2-Selmer group, this provides an upper bound for the rank of $J(\mathbf{Q})$. The descent process can be continued, though with somewhat greater difficulty; for 4-descents see [11]. One can also carry out 2-descents for the more general elliptic curve

$$Y^2 = X^3 + aX^2 + bX + c;$$

but in order to do this one requires information about the splitting field of the right hand side.

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 in 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. (See [16].) 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 ([18] and [19]) have shown that this point has infinite order precisely when $L'(1, J) \neq 0$. Building on their work, Kolyvagin (see [17]) has shown the following.

Theorem 2 *Suppose that the Heegner point has infinite order; then the group $J(\mathbf{Q})$ has rank 1 and $Ш(J)$ is finite.*

Kolyvagin [25] has also obtained sufficient conditions for both $J(\mathbf{Q})$ and $Ш(J)$ to be finite. The following result is due to Nekovar and Plater.

Theorem 3 *If the order of $L(s, J)$ is odd then either $J(\mathbf{Q})$ is infinite or the p-part of $Ш(J)$ is infinite for every good ordinary p.*

If J can be parametrized by modular functions for some arithmetic subgroup of $\mathrm{SL}_2(\mathbf{R})$ then analytic continuation and the functional equation 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 *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 $Ш(J)$ 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 [31]. 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 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 $Ш(J)$ 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 Ш with values in $\mathbf{Q}/\mathbf{Z}$, which is nonsingular on the quotient of Ш by its maximal divisible subgroup. Thus finiteness implies that if 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 3 *Suppose that* $Ш(J)$ *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.*

This result will play a crucial role in §§6 and 7.

5. *Generalities about surfaces.*
Over $\mathbf{C}$ a full classification of surfaces can be found in [1]. A first coarse classification is given by the *Kodaira dimension* κ, which for surfaces can take the values $-\infty, 0, 1$ or 2. What also seems to be 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 in §6; in this case the Diophantine problems for V are only of interest when $C(K)$ is nonzero, in which case 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 $\mathbf{C}$.

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 §2.

In the next two sections I shall outline what can at present be said about rational surfaces and K3 surfaces respectively; these appear to be the two most interesting families of surfaces for the number-theorist. In both cases many of the most recent results depend on one or both of two major conjectures. One of these (for the reason given near the end of §4) is the finiteness of the Tate-Shafarevich group; the other is Schinzel's Hypothesis, which we now describe. It 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 split in $\mathbf{Z}[X]$.
- There may be a prime p such that for any value of x mod p at least one of the $F_i(x)$ is divisible by p.

Clearly the second obstruction can only happen for $p \leq \sum \deg(F_i)$. 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. There are various more complicated variants of this hypothesis (including ones in other algebraic number fields), but they all follow fairly easily from the hypothesis in its original form.

No one in his right mind would attempt to prove Schinzel's Hypothesis; indeed one instance is the notoriously intractable twin primes problem, which is the special case when the F_i are the two polynomials $X + 1$ and $X - 1$. But probabilistic arguments suggest that the hypothesis is in fact true. At the very least it would be perverse to look for counter-examples to results which have been proved subject to Schinzel's Hypothesis.

6. *Rational surfaces.*

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. 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 no aesthetic merits and have attracted little attention; it seems sensible 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.

We consider first pencils of conics, and assume that (5) is defined over $\mathbf{Q}$, the argument for an arbitrary algebraic number field not being essentially different. We can require the coefficients of the $a_i(u,v)$ to be in $\mathbf{Z}$. Since the Hasse principle holds for conics, it is enough to choose $u = u_0, v = v_0$ in such a way that (5) is locally soluble at $2, \infty$ and all the odd primes which divide any of the $a_i(u_0, v_0)$. As it stands, this appears to involve arguing in a circle; the way to make the argument respectable is as follows.

Assume that (5) is everywhere locally soluble. By absorbing suitable factors into the X_i, we can ensure that the $a_i(u,v)$ are square-free and coprime. To achieve this, we have to drop the condition that the $a_i(u,v)$ are all of the same degree; but it is still true that their degrees are all even or all odd. Denote by $\mathcal{B}$ the set of bad places, which turns out to consist of $2, \infty$, the primes which divide the discriminant of $a_0(u,v)a_1(u,v)a_2(u,v)$ and the primes which do not exceed the degree of that product. Let $\mathcal{S}$ be the space of all pairs of coprime integers u_0, v_0, with the topology induced by the places of $\mathcal{B}$; and let $\mathcal{S}_0$ be the subset of $\mathcal{S}$ consisting of the points at which (5) is locally soluble at every place in $\mathcal{B}$. By hypothesis, $\mathcal{S}_0$ is not empty; and it is

open in $\mathcal{S}$. To obtain solubility in $\mathbf{Q}$, we have to choose u_0, v_0 in $\mathcal{S}_0$ so that (5) is locally soluble at each good prime p_0 which divides one of the $a_i(u_0, v_0)$; for solubility at the other good primes is trivial, and we have already taken care of the bad places. Let $c(u, v)$ be the irreducible factor of that one of the $a_i(u, v)$ for which $p_0|c(u_0, v_0)$, and to fix ideas assume that $c(u, v)$ divides $a_2(u, v)$; here $c(u, v)$ is unique because p_0 does not divide the discriminant of $a_0a_1a_2$. The condition of local solubility at p_0 is

$$(a_0(u_0, v_0)a_1(u_0, v_0), c(u_0, v_0))_{p_0} = +1 \tag{6}$$

where the outer bracket is the Hilbert symbol. So a necessary condition for the solubility of (5) is that all the conditions like

$$\prod (a_0(u_0, v_0)a_1(u_0, v_0), c(u_0, v_0))_p = +1 \tag{7}$$

hold simultaneously for some (u_0, v_0) in $\mathcal{S}_0$, where the product is taken over all p which divide $c(u_0, v_0)$.

What is unexpected is that this turns out to be useful, because of the following lemma. The proof of the lemma is straightforward, since the function Φ behaves like a quadratic residue symbol and can be evaluated by a Euclidean algorithm process very like that which is used for such symbols.

Lemma 4 *Let $F(u, v), G(u, v)$ be homogeneous polynomials in $\mathbf{Z}[u, v]$, with $\deg(F)$ even. Let $\mathcal{B}$ be a finite set of places of $\mathbf{Q}$ which contains $2, \infty$ and all the primes which divide the discriminant of FG. For any coprime u_0, v_0 in $\mathbf{Z}$, write*

$$\Phi(\mathcal{B}; F, G; u_0, v_0) = \prod (F(u_0, v_0), G(u_0, v_0))_p \tag{8}$$

where the outer bracket on the right is the Hilbert symbol and the product is taken over all primes p not in $\mathcal{B}$ such that $p|G(u_0, v_0)$. Then $\Phi(u_0, v_0)$ is continuous in the topology on $\mathcal{S}$, and computable.

In this result we take $F = a_0a_1, G = c$; we noted above that $\deg(a_0a_1)$ is necessarily even. It follows that a necessary condition for the solubility of (5) is that there is a point (u_0, v_0) in $\mathcal{S}_0$ such that $\Phi(u_0, v_0) = +1$ for all Φ which can be generated from (5) in this way. This condition is computable, and it is unsurprising (though not obvious) that it turns out to be equivalent to the Brauer-Manin condition for (5).

If one assumes Schinzel's Hypothesis, this condition is also sufficient. For suppose that u_0, v_0 have been so chosen that there is only one good prime p_0

which divides $c(u_0, v_0)$; then the product in (7) reduces to the left hand side of (6), and so (6) holds for this prime. Now choose an open set $\mathcal{N} \subset \mathcal{S}_0$ such that (7) holds throughout $\mathcal{N}$ for each $c(u, v)$; by a slightly modified version of Schinzel's Hypothesis we can choose (u_0, v_0) in $\mathcal{N}$ so that every $c(u_0, v_0)$ is the product of one good prime and possibly some factors in $\mathcal{B}$. As c runs through all irreducible factors of $a_1a_2a_3$, p_0 runs through all those primes for which we have to verify (6). Thus (5) is everywhere locally soluble for the pair u_0, v_0, and therefore globally soluble. With minor modifications, the same argument shows that (subject to Schinzel's Hypothesis) the Brauer-Manin obstruction is also the only obstruction to weak approximation.

If there is no Brauer-Manin obstruction, this construction finds infinitely many conics in the pencil which contain rational points. But, somewhat unexpectedly, even if we know some conics of the pencil which are soluble, without Schinzel's Hypothesis we do not know how to generate more such conics.

Question 12 *Given a pencil of conics and finitely many conics in the pencil each of which contains rational points, can we generate further conics of the pencil which contain rational points without using Schinzel's Hypothesis?*

If we know even one rational point on a Del Pezzo surface V of degree 3 or 4, we can obtain an infinity of curves of genus 0 each of which lies on V, though they will be singular and for degree 3 it will usually not be true that each point of $V(\mathbf{Q})$ lies on at least one curve of the family. But without such a point, the best we can do is to find on V a family of curves of genus 1. At first sight, it would seem that in these circumstances nothing resembling the argument above can be applied; for an essential component of that argument was that conics satisfy the Hasse principle, and this is not true for curves of genus 1. However Lemma 3 provides us with a way round this obstacle.

The arguments involved are applicable to some surfaces V which are not necessarily rational, but which are elliptic with a fibration $V \to \mathbf{P}^1$. Consider a pencil of curves $\mathcal{C}_\lambda$ of genus 1, each of which is a 2-covering of its Jacobian J_λ. If we can choose λ in such a way that $\mathcal{C}_\lambda$ is everywhere locally soluble and at least half the elements of the 2-Selmer group of J_λ are soluble (and if we assume the finiteness of the relevant Tate-Shafarevich group), then it will follow from Lemma 3 that $\mathcal{C}_\lambda$ is soluble. For this machinery to have any chance of working, we must be able to implement the 2-descent on J_λ in a manner which is uniform in λ. This more or less requires J_λ to have its

2-division points defined over $\mathbf{Q}(\lambda)$ and therefore to have the form

$$Y^2 = (X - c_1(\lambda))(X - c_2(\lambda))(X - c_3(\lambda)) \tag{9}$$

where the $c_i(\lambda)$ are in $\mathbf{Q}(\lambda)$; but an additional trick, given in [2], enables the method to be used even if J_λ has just one 2-division point in $\mathbf{Q}(\lambda)$.

The details of this method are unattractive, but the strategy is as follows. (For a full account, see [13].) Without loss of generality we can assume that the $c_i(\lambda)$ are in $\mathbf{Z}[\lambda]$. For any particular integral value λ_0 of λ, the bad places for the equation (9) are the bad places for the system together with the primes which divide one of the $c_i(\lambda_0) - c_j(\lambda_0)$. It was explained in §4 how to implement the 2-descent for (9). We shall eventually use Schinzel's Hypothesis to choose λ_0 so that the value of each irreducible factor of any $c_i(\lambda) - c_j(\lambda)$ at $\lambda = \lambda_0$ is the product of some bad primes for the system with one good prime. We call the latter a *Schinzel prime*; though it is a good prime for the system, it is a bad prime for the curve obtained by writing $\lambda = \lambda_0$ in (9). The effect of restricting λ_0 in this way is that we know those 2-coverings of (9) for $\lambda = \lambda_0$ which are locally soluble at all good primes for the curve; they form a finite group of 2-coverings $\mathcal{C}'_\lambda$ of J_λ which does not depend on the choice of λ_0 provided it satisfies the condition above.

This group certainly contains the original $\mathcal{C}_\lambda$ and the 2-coverings which correspond to the 2-division points. The next step, which involves a sophisticated analysis of the 2-descent process and also requires us to introduce additional well chosen bad primes for the system, is to find local conditions on λ_0 at the bad primes of the system which ensure that for $\lambda = \lambda_0$

- the only elements of this group which are locally soluble at all the bad places of the system lie in the subgroup generated by the original $\mathcal{C}_\lambda$ and the 2-coverings generated by the 2-division points; and
- the original $\mathcal{C}_\lambda$ is locally soluble at all the bad places of the system.

This is not always possible; if it is impossible, that provides an obstruction to this method of attack on the problem though not necessarily to the solubility of the system. In general this obstruction is not much stronger than the Brauer-Manin obstruction, and in some cases they are provably the same; so this is not too serious a blemish on the method. If we achieve the two properties above then solubility at the Schinzel primes turns out to be automatic. (This is an example of what seems to be a rather general phenomenon, that if

one thing goes wrong, so must at least one other which is related to it.) With our enlarged set of bad places for the system, we now choose λ_0 to satisfy the local conditions and the Schinzel condition in the previous paragraph. By Lemma 3, the curve (9) is soluble for this value of λ. But in contrast to what happens for pencils of conics, this kind of argument appears to provide no information about weak approximation.

Question 13 *Can one modify the method above so that it works without any assumption about the* 2*-division points of* J_λ*?*

Unfortunately it is not known (and probably is not even true) that an arbitrary Del Pezzo surface of degree 4 contains a pencil of curves of genus 1 of this particular type — and the situation for Del Pezzo surfaces of degree 3 is much worse, in that the natural curves to consider are 3-coverings rather than 2-coverings.

However, for Del Pezzo surfaces of degree 4 some progress has been made. Salberger and Skorobogatov [33] have shown that the Brauer-Manin obstruction is the only obstruction to weak approximation. (Recall that weak approximation presupposes the existence of at least one rational point.) As for the Hasse principle, the present situation is as follows. A Del Pezzo surface of degree 4 defined over the algebraic number field K has the form

$$V : F_1(X_0, \ldots, X_5) = F_2(X_0, \ldots, X_5) = 0,$$

where the F_1 and F_2 are homogeneous quadratic and their coefficients are in K. By a linear transformation defined over an extension K_1 of odd degree over K, we can separate off one of the variables; and over K_1 we can find a pencil of curves $\mathcal{C}_\lambda$ of genus 1 on V for which each J_λ has one 2-division point defined over $K_1(\lambda)$. Using the trick described in [2], and subject to an obstruction typical for the method, it can now be shown that V contains a point defined over K_1. A straightforward geometric argument, which does not rely on K being an algebraic number field, now shows that V contains a point defined over K. Unfortunately the overall arguments are so complicated (and so unnatural) that it is not clear whether the obstruction to the method is still simply the Brauer-Manin obstruction to the solubility of V over K; but even if it is stronger, it is not much stronger.

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 *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. 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.

A variant of the method above can be applied to diagonal cubic surfaces

$$V : a_0X_0^3 + a_1X_1^3 = a_2X_2^3 + a_3X_3^3, \tag{10}$$

subject to one very counterintuitive condition, which is that K, the field of definition of V, must not contain the primitive cube roots of unity. Write V in the form

$$a_0X_0^3 + a_1X_1^3 = \lambda Y^3, \quad a_2X_2^3 + a_3X_3^3 = \lambda Y^3 \tag{11}$$

where λ is at our disposal. We now have two pencils of curves of genus 1, each of which is a $\sqrt{-3}$-covering of its Jacobian; and we have to apply the method simultaneously to both curves. This introduces considerable additional complications, for which see [44]; and the obstruction to the method, though weak, is certainly strictly stronger than the Brauer-Manin obstruction. The reason for the condition on K is that otherwise the curves (11) would admit complex multiplication, and the latter acts on the $\sqrt{-3}$-Selmer groups; thus the order of the latter would always be an odd power of 3, whereas it has to be reduced to 9 for the method to work. (Here one factor 3 arises because of the 3-division points on the Jacobian defined over $\mathbf{Q}(\sqrt{-3})$.) On the other hand, in this argument we only need apply Schinzel's Hypothesis to the single polynomial X, so that it can be replaced by Dirichlet's theorem on primes in arithmetic progression.

All this relates to Question (A). For Question (B) the only known results are for quadrics, for which see the remarks after Theorem 1. It seems reasonable to ask whether there is an analogous result for other kinds of rational surfaces; this is another problem for which the first step should probably be to use numerical search to generate a plausible conjecture. For this purpose, one needs to examine a system with not too many parameters; and this leads to the following question:

Question 15 *For the surface V given by* (10) *with the a_i in $\mathbf{Z}$, is there a polynomial P in the $|a_i|$ such that if V is soluble in $\mathbf{Z}$ then it has such a solution for which each summand is absolutely bounded by P?*

The ideal answer to Question (C) would be to provide a birational map $V \to \mathbf{P}^2$ defined over $\mathbf{Q}$. However, it can be shown that such a map exists for nonsingular cubic surfaces V if and only if $V(\mathbf{Q})$ is not empty and V contains a divisor defined over $\mathbf{Q}$ which consists of 2, 3 or 6 skew lines. (For Del Pezzo surfaces of degree 4, the second condition must be replaced by the statement that V contains a divisor defined over $\mathbf{Q}$ which consists of one or more skew lines.) For Châtelet surfaces, which have the form

$$X_2(X_0^2 - cX_1^2) = f(X_2, X_3)$$

where c is a non-square and f is homogeneous cubic, it is known (see [12]) that there is a finite set of parametric solutions (each in 4 inhomogeneous variables) such that each point of $V(\mathbf{Q})$ is represented by one of them, though in an infinity of different ways. But in general more than one parametric solution is needed, and it was already shown in [26] that parametric solutions in only 2 variables cannot play a useful part in the process.

Question 16 *Is there a larger class of cubic surfaces (ideally, the class of all nonsingular cubic surfaces) for which analogous results hold?*

The question of parametric solutions is linked to the idea of *R-equivalence*. Let V be a variety defined over $\mathbf{Q}$; then R-equivalence is defined as the finest equivalence relation such that two points given by the same parametric solution are equivalent. Alternatively, it is the finest equivalence relation such that for any map $f : \mathbf{P}^1 \to V$ and points P_1, P_2, all defined over $\mathbf{Q}$, the points $f(P_1)$ and $f(P_2)$ are equivalent. A good deal is known about R-equivalence on cubic surfaces; in particular, it is shown in [43] that the closure of an R-equivalence class in $V(\mathbf{A})$ is computable, and that the closures of two R-equivalence classes are either the same or disjoint. There is an example in [12] of a Châtelet surface V containing two distinct R-equivalence classes, each of which has the whole of $V(\mathbf{A})$ as its closure. Work of Coray and Tsfasman shows that this V is birationally equivalent to a nonsingular cubic surface.

Question 17 *Is the set of R-equivalence classes on a nonsingular cubic surface finite?*

7. K3 *surfaces and Kummer surfaces.*
K3 surfaces are the simplest kind of variety about whose number-theoretic

properties very little is known; indeed they still present many unsolved problems even to the geometer. There are infinitely many families of K3 surfaces; the simplest of them, and the only one which will be considered in the present article, consists of all nonsingular quartic surfaces in $\mathbf{P}^3$. An important special type of K3 surfaces consists of the *Kummer surfaces*, a phrase which can carry either of two related meanings:

- The quotient of an Abelian surface A by the automorphism -1; this has 16 singular points corresponding to the 16 2-division points of A.
- The nonsingular surface obtained by blowing up the 16 singular points in the previous definition.

One advantage of Kummer surfaces in comparison with general K3 surfaces is that for the former it is easy to determine $\mathrm{Pic}(\bar{V})$.

Some K3 surfaces contain one or more pencils of curves of genus 1, and these pencils may even be of the kind discussed in the previous section; but one should not confine one's attention to K3 surfaces with this additional property. For the time being, there is merit in concentrating on diagonal quartics

$$V : a_0X_0^4 + a_1X_1^4 + a_2X_2^4 + a_3X_3^4 = 0, \tag{12}$$

because these contain few enough parameters to make systematic numerical experimentation possible. However, the number theory of such surfaces may be exceptional, because the geometry certainly is. Indeed $\mathrm{Pic}(\bar{V})$ has rank 20, which is the largest possible value for any K3 surface, and it is generated by the classes of the 48 lines on $\bar{V}$; moreover V is a Kummer surface up to isogeny, and indeed is the Kummer surface of $E \times E$ where E is a certain elliptic curve which admits complex multiplication. One consequence of this is that V is rigid in the sense of algebraic geometry.

There is an obvious map from V to the quadric surface

$$W : a_0Y_0^2 + a_1Y_1^2 + a_2Y_2^2 + a_3Y_3^2 = 0.$$

If $a_0a_1a_2a_3$ is a square, and V is everywhere locally soluble, each of the two families of lines on W is defined over the ground field, and each such line lifts to a curve of genus 1 on V; moreover the Jacobians of these curves have the form (9), so that the methods of the previous section can be applied.

Martin Bright [7] has computed and tabulated $\mathrm{Br}_1(V)/\mathrm{Br}(\mathbf{Q})$ for all V of the form (12); it is necessary to do this by computer, because there are

546 distinct cases. Assuming Schinzel's Hypothesis and the finiteness of Ш, I had previously shown in [42] that over $\mathbf{Q}$ the Brauer-Manin obstruction is the only obstruction to the Hasse principle in the most general case in which $a_0a_1a_2a_3$ is a square. (Most general in this context means that none of the $\pm a_ia_j$ is a square and $a_0a_1a_2a_3$ is not a fourth power.) It seems reasonable to hope that the same property will still hold in all the cases for which $a_0a_1a_2a_3$ is a square; but there are too many of them to examine individually. On the other hand, there is strong numerical evidence that when $a_0a_1a_2a_3$ is not a square the obstruction coming from $\mathrm{Br}_1(V)$ is not in general the only obstruction to the Hasse principle.

Question 18 *What is the additional obstruction in this case?*

One particularly interesting example is the surface

$$X_0^4 + 2X_1^4 = X_2^4 + 4X_3^4; \tag{13}$$

this has two obvious rational points, but appears to have no others.

8. *Density of rational points.*
So far I have ignored Question (D). It differs from the others in that it is not a birational question, but is associated with a particular embedding of the variety V in projective space. For simplicity we work over $\mathbf{Q}$. A point P in $\mathbf{P}^n$ defined over $\mathbf{Q}$ has a representation $(x_0, \dots, x_n)$ 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 $\max|x_i|$; 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

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

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 [3].

Theorem 5 *Let $r_1, \ldots, r_m$ be positive odd integers, not necessarily all different. Then there exists $N_0(r_1, \ldots, r_m)$ with the following property. For any $N \geq N_0$ let $F_i(X_0, \ldots, X_N)$ be homogeneous polynomials with coefficients in $\mathbf{Z}$ and $\deg F_i = r_i$ for $i = 1, \ldots, m$. Then the F_i have a common nontrivial zero in $\mathbf{Z}^N$.*

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 totally complex algebraic number field there is a similar theorem for which the r_i can be any positive integers.

Question 19 *In Theorem 5, can the condition that all the r_i are odd be replaced by the requirement on the F_i that the projective variety given by $F_1 = \ldots = F_m = 0$ has a nonsingular real point?*

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 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 [22] is the most impressive result in this direction.

Theorem 6 *Homogeneous nonsingular nonary cubics over $\mathbf{Q}$ satisfy both the Hasse principle and weak approximation.*

It appears that the Hardy-Littlewood method can only 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. 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. For simplicity, we describe his conjecture only for Del Pezzo surfaces V of degrees 3 and 4. To ask about $N(H, V)$ is now 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. For the latter suggests an estimate $AH \prod(N(p)/(p+1))$, where the product is taken over all primes less than a certain bound which depends on H. In view of what is said in §3, this product ought to be replaced by something which depends on the behaviour of $L_2(s, V)$ near $s = 1$. More precisely, 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 (14) as a conjectural estimate for $N(H, V)$. But if this argument were valid, L would contain more rational points than V, even though $V \supset L$. 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 27 or 16 lines on V. Manin conjectured that

$$N(H, U) \sim AH(\log H)^{r-1} \text{ where } r \text{ is the rank of } \mathrm{Pic}(V); \qquad (14)$$

and Peyre [28] has given a conjectural formula for A. (But note that there exist Fano varieties of dimension greater than 2 for which (14) is certainly false; and it is not clear how Manin's conjecture should be modified to cover such cases.) Various people have proved this conjecture for the cone $X_0X_1X_2 = X_3^3$, and there are also results for the singular cubic surface

$$X_0X_1X_2 + X_0X_1X_3 + X_0X_2X_3 + X_1X_2X_3 = 0,$$

to which attention had been drawn by Birch. Heath-Brown [21] has proved that

$$A_1H(\log H)^6 < N(H, U) < A_2H(\log H)^6$$

for suitable constants A_1, A_2; but he doubts whether his method is capable of proving an asymptotic formula. Using quite different ideas, Rudge has sketched a proof of the asymptotic formula; but the details are not yet complete.

Question 20 *Are there nonsingular Del Pezzo surfaces of degree* 3 *or* 4 *for which the Manin conjecture can be proved?*

In the first instance, it would be wise to address this problem under rather restrictive hypotheses about $\mathrm{Pic}(V)$, 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. A one-sided estimate for one such family is given in [39].

For Del Pezzo surfaces, the 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 21 *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. But K3 surfaces pose new problems — and not ones on which any practicable amount of computation is likely to shed light. If V is a K3 surface, then we have to study not $N(H,V)$ but $N(H,U)$ where U is obtained from V by deleting the curves of genus 0 on V defined over $\mathbf{Q}$, of which there may be an infinite number. One can expect that $N(H,U) \sim A(\log H)^c$ for some constants A and c; and it seems reasonable to hope that c will be a half-integer. The surface (13) suggests that we can have $c = 0$, and it must be certain (though perhaps difficult to prove) that c can sometimes be strictly positive.

Question 22 *Can the value of c be obtained from the L-series $L_2(s, V)$?*

Question 23 *If V is a Kummer surface obtained from the Abelian surface A, is c related to the rank of the Mordell-Weil group of A?*

I am indebted to Jean-Louis Colliot-Thélène for many valuable comments; but he bears no responsibility for the opinions expressed.

REFERENCES

[1] A.Beauville, *Complex Algebraic Surfaces* (2nd ed., Cambridge, 1996).
[2] A.O.Bender and 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. London Math. Soc (3) 83(2001), 299-329.
[3] B.J.Birch, Homogeneous forms of odd degree in a large number of variables, Mathematika 4(1957), 102-105.
[4] S.J.Bloch, *Higher regulators, algebraic K-theory and zeta-functions of elliptic curves*, CRM Monograph Series 11 (AMS, 2000).
[5] S.J.Bloch and K.Kato, L-functions and Tamagawa numbers of motives, in *The Grothendieck Festschrift*, vol. I, pp. 333-400 (Birkhauser, 1990).
[6] A.Borel, Cohomologie de SL_2 et valeurs de fonctions zeta aux points entiers, Ann. Sc. Norm. Pisa (1976), 613-636.
[7] M.Bright, Ph.D. dissertation, (Cambridge, 2002).
[8] M.Bright and Sir Peter Swinnerton-Dyer, Computing the Brauer-Manin obstructions, Math. Proc. Cambridge Phil. Soc. (to appear).
[9] *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry* (ed. Jan Denef et al), Contemporary Mathematics, vol. 270.
[10] *Mathematical Developments arising from Hilbert Problems*, AMS Symposia in Pure Mathematics, Vol XXVIII (ed. F.E.Browder), (Providence, 1976).
[11] J.W.S.Cassels, Second descents for elliptic curves, J. reine angew. Math. 494(1998), 101-127.
[12] J-L.Colliot-Thélène, J-J.Sansuc and Sir Peter Swinnerton-Dyer, Intersections of two quadrics and Châtelet surfaces, J. reine angew. Math. 373(1987), 37-107 and 374(1987), 72-168.
[13] J-L.Colliot-Thélène, A.N.Skorobogatov and Sir Peter Swinnerton-Dyer, Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points, Invent. Math. 134(1998), 579-650.

[14] J-L.Colliot-Thélène and Sir Peter Swinnerton-Dyer, Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties, J. Reine Angew. Math., 453(1994) 49-112.
[15] *Rational Points*, ed. G.Faltings and G. Wüstholz (3rd ed., Vieweg, 1992).
[16] J.Gebel and H.G.Zimmer, Computing the Mordell-Weil Group of an Elliptic Curve over $\mathbf{Q}$, in *Elliptic Curves and Related Topics* (ed. H.Kisilevsky and M. Ram Murthy), CRM Proceedings and Lecture Notes, vol 4, pp 61-83 (Amer. Math. Soc., 1994).
[17] B.Gross, Kolyvagin's work on modular elliptic curves, in *L-functions and Arithmetic* ed. J.Coates and M.J.Taylor (Cambridge, 1991).
[18] B.Gross, W.Kohnen and D.Zagier, Heegner points and derivatives of L-series II, Math. Ann. 278(1987), 497-562.
[19] B.Gross and D.Zagier, Heegner points and derivatives of L-series, Invent. Math. 84(1986), 225-320.
[20] D.Harari, Obstructions de Manin "transcendantes", in *Séminaire de Théorie des Nombres de Paris 1993-1994*, ed. S.David, (Cambridge, 1996).
[21] D.R.Heath-Brown, The Density of Rational Points on Cayley's Cubic Surface, (unpublished).
[22] C.Hooley, On nonary cubic forms, J. Reine Angew. Math., 386(1988), 32-98 and 415(1991), 95-165 and 456(1994), 53-63.
[23] W.W.J.Hulsbergen, *Conjectures in Arithmetic Algebraic Geometry*, (Vieweg, 1992).
[24] S.L.Kleiman, Algebraic cycles and the Weil conjectures, in *Dix exposés sur la cohomologie des schémas*, ed. A.Grothendieck and N.H.Kuiper (North-Holland, 1968).
[25] V.A.Kolyvagin, Finiteness of $E(\mathbf{Q})$ and $Ш(E/\mathbf{Q})$ for a class of Weil curves, Izv. Akad. Nauk SSSR 52(1988).
[26] Yu.I.Manin, *Cubic Forms*, (North-Holland, 1974).
[27] B.Mazur, Rational isogenies of prime degree, Inv. Math. 44(1978), 129-162.
[28] E.Peyre, Hauteurs et mesures de Tamagawa sur les variétés de Fano, Duke Math. J. 79(1995), 101-218.
[29] S.Raghavan, Bounds for minimal solutions of Diophantine equations, Göttinger Nachr. (1975), 109-114.
[30] *Beilinson's Conjectures on Special Values of L-Functions*, ed. M.Rapaport, N.Schappacher and P.Schneider (Academic Press, 1988).
[31] K.Rubin, Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton-Dyer, in *Arithmetic Theory of Elliptic Curves*

(ed. C.Viola), pp. 167-234 (Springer Lecture Notes 1716 (1999)).
[32] K.Rubin and A.Silverberg, Ranks of Elliptic Curves, Bull. Amer. Math. Soc. 39(2002), 455-474.
[33] P.Salberger and A.N.Skorobogatov, Weak approximation for surfaces defined by two quadratic forms, Duke J. Math. 63(1991), 517-536.
[34] J-P.Serre, Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures), Séminaire Delange-Pisot-Poitou 1969/70, exp. 19.
[35] C.L.Siegel, Normen algebraischer Zahlen, (Werke, Band IV, 250-268).
[36] A.Silverberg, Open Questions in Arithmetic Algebraic Geometry, in *Arithmetic Algebraic Geometry* pp. 85-142 (AMS, 2002)
[37] A.N.Skorobogatov, Beyond the Manin obstruction, Inv. Math. 135(1999), 399-424.
[38] A.N.Skorobogatov, *Torsors and Rational Points*, (Cambridge, 2002).
[39] J.B.Slater and Sir Peter Swinnerton-Dyer, Counting points on cubic surfaces I, Astérisque 251(1998), 1-11.
[40] P.Swinnerton-Dyer, The Conjectures of Birch and Swinnerton-Dyer, and of Tate, in *Proceedings of a Conference on Local Fields* (ed. T.A.Springer), Driebergen 1966, pp. 132-157 (Springer, 1967).
[41] Sir Peter Swinnerton-Dyer, Rational points on pencils of conics and on pencils of quadrics, J. London Math. Soc. (2) 50(1994), 231-242.
[42] Sir Peter Swinnerton-Dyer, Arithmetic of diagonal quartic surfaces II, Proc. London Math. Soc. (3) 80(2000), 513-544.
[43] Sir Peter Swinnerton-Dyer, Weak approximation and R-equivalence on Cubic Surfaces, in *Rational points on algebraic varieties* (ed. E.Peyre and Y.Tschinkel) pp. 357-404 (Birkhäuser, 2001).
[44] Sir Peter Swinnerton-Dyer, The solubility of diagonal cubic surfaces, Ann. Scient. Éc. Norm. Sup. (4) 34(2001), 891-912.
[45] J.T.Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, Sém. Bourbaki 306(1966).
[46] R.C.Vaughan, *The Hardy-Littlewood method*, (2nd ed., Cambridge, 1997).
[47] L.Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Invent. Math. 124(1996), 437-449.