BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 14, Number 2, April 1986

ARITHMETIC ON CURVES

BY BARRY MAZUR

CONTENTS

I. **What are Diophantine problems?**
1. Miscellaneous Diophantine problems
2. Systematic formulations
3. Digression: Questions of integral solutions vs. Questions of Diophantine approximations

II. **Curves**
1. Plane curves
2. Algebraic curves
3. Smooth curves
4. Riemann surfaces
5. Simplifying the singularities of a plane curve
6. Genus
7. The fundamental trichotomy
8. Interlude: A geometric finiteness result
9. On Mordell's conjecture and its analogue

III. **Jacobians and abelian varieties**
1. An extension of the chord-and-tangent method to curves of genus $\geqslant 2$: The jacobian of a curve
2. The analytic parametrization of J by algebraic integrals modulo periods
3. The algebraic nature of the jacobian
4. The arithmetic nature of the jacobian

IV. **Classification of families with bounded bad reduction**
1. Kodaira's problem
2. Shafarevich's problems
3. Parshin's construction: Shafarevich's conjecture implies Mordell's conjecture

V. **Heights**
1. Height of points
2. Normed vector spaces
3. Heights of abelian varieties
4. A block diagram

Received by the editors June 12, 1985.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 14Hxx, 14Kxx, 11Dxx, 00-01, 01-01, 01A65, 11-01, 11G05, 11G10, 11G15.

Bibliography

1. General references
2. References requiring some background
3. Accounts of the proof of Mordell's conjecture which require familiarity with the techniques of number theory or algebraic geometry
4. Other works cited (given in alphabetical order)

I. WHAT ARE DIOPHANTINE PROBLEMS?

I don't know the answer. To feel our way around the question, let us first consider some miscellaneous problems that have been labelled "Diophantine" and then review some attempts towards a systematic organization of these "Diophantine problems".

The point of such a preamble is to get us to appreciate why number-theorists are often so fondly devoted to the study of rational points on algebraic curves, and to sense the more general contexts which embrace that study.

My aim will then be to discuss the recent progress made in the arithmetic of curves [**Fa**]′,[1] and to explain a few of the ideas involved without requiring substantial background in algebra, number theory, or algebraic geometry.

This survey has been culled from my notes to the Colloquium Series Lectures at the 1984 winter meeting of the American Mathematical Society at Louisville, Kentucky, and from part of the Albert Lectures delivered at the University of Chicago this past fall. I feel very lucky to have had such engaging and stimulating audiences.

I am very appreciative of the comments and suggestions of J.-P. Serre who read closely early versions of this survey. I am also thankful for the help and advice I received from many people in the course of writing it, among whom are: Mike Artin, Greg Call, Persi Diaconis, John Hsia, John Hubbard, Nick Katz, Serge Lang, Joe Mazur, David Mumford, Julia Robinson, Joe Silverman, John Tate, Jeremy Teitelbaum, and Don Zagier.

1. Miscellaneous Diophantine problems.

(a) [Chosen at random from Diophantus] (V.16) *Find three numbers such that when each is subtracted from the cube of their sum, a cube remains.*

(b) [Diophantine approximation (of irrationals)] Since $\sqrt{2}$ is irrational, $x^2 - 2y^2$ never represents 0 for integral values of x and y, not both zero. But, for such values of x and y, $x^2 - 2y^2$ is integral, and therefore the smallest values it can assume are

$$x^2 - 2y^2 = \pm 1$$

which is a type of equation that is universally (but wrongly, it turns out [**Wl**]′) referred to as a *Pellian equation*.[2]

[1] A *prime* after a reference (e.g. [**Fa**]′) indicates that it is to be found in one of the first three sections of the bibliography.

[2] The *Archimedes Cattle Problem* also reduces to Pell's equation. See [**Wl, Fo**]′ for very readable accounts of this.

Weil [**Wl**]′ provides a beautiful account of the treatment that the Pellian equation received in the

Such an equation has been known since the 17th century to have an *infinity* of integral solutions

x	y	x/y
1	1	1.0
3	2	1.5
7	5	1.4
17	12	1.416 ⋯
41	29	1.4137 ⋯
99	70	1.41428 ⋯
239	169	1.414201 ⋯
577	408	1.414215 ⋯
1393	985	1.4142132 ⋯
3363	2376	1.4142136 ⋯
⋮	⋮	⋮

and as the size of y increases, x/y provides better and better approximations to $\sqrt{2}$. Specifically, since

$$(x/y)^2 - 2 = \pm 1/y^2,$$

one can easily find a constant c (e.g., $c = 1$) such that

$$|x/y - \sqrt{2}| \leqslant c/y^2,$$

for all pairs (x, y) on our list. In fact, in a technical sense the above list is the complete collection of "best approximants" to $\sqrt{2}$.

There may be something daunting about being confronted with an "infinity" of different solutions to the same Diophantine problem. But for any Pellian equation and for this one in particular, all solutions (x, y) may be obtained systematically from the smallest one, the rule being in this case

$$x + \sqrt{2}y = (1 + \sqrt{2})^N$$

hands of the Indian mathematicians Brahmegupta (7th century A.D.) and Bhascara (12th century A.D.). They dealt with the general equation written in modern terms in the display below, each ingredient of which was known by its particular name (whose rough English translation is indicated)

$$\overset{\text{major root}}{X}{}^2 - \underset{\text{qualifier}}{A} \cdot \overset{\text{minor root}}{Y}{}^2 = \underset{\text{additive}}{m}.$$

The multiplicative property of solutions was known by the name "bhāvanā" which apparently means "production rules". The Indian mathematicians also had a process known as "kuṭṭaka" (or: "the pulverizer") which brought, in effect, the Euclidean algorithm to bear on the problem of producing new solutions from old. Bhascara and earlier mathematicians were also aware of the fact that all solutions for $m = \pm 1$ come from the smallest solution; the process enabling one to generate all from the smallest went under the name "cakravāla" (from *cakra* = a wheel).

where N runs systematically through all integers.[3]

To what extent does the optimistic extension of this principle hold? Is it the case that whenever there are an infinity of solutions to a given Diophantine question, there is some systematic coherence to this infinite collection, which enables us in an orderly way to generate all of them from a finite subcollection?

(c) [From geometry]

—The famous *Pythagorean problem* of listing all right-angle triangles all of whose sides are integral was solved in antiquity.

—The *Congruence number problem* (which dates, apparently, to an Arab manuscript of the 10th century) is to determine for a given natural number n whether there exists a right-angle triangle with all three sides rational and area equal to n (such a number n is called *congruent*).

Two years ago, using a host of modern equipment (the arithmetic of elliptic curves, L-functions, modular forms of half-integral weight) Tunnell produced a beautiful and simple algorithm which (if a standard conjecture in the theory of elliptic curves were true) would determine all congruent numbers. For example, for odd integers n, Tunnell's algorithm simply requires you to check whether the number of triples (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = n$ is twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = n$ (conjecturally, an odd integer n is congruent if and only if this happens).[4]

—Let $W \subset \mathbf{C}^2$ be an algebraic plane curve. That is, W is the locus of zeroes of a polynomial in two variables with complex coefficients. Is it possible that there be an infinity of points on W all expressible as rational linear combinations of a finite number of points in the plane $\mathbf{C}^2$?[5]

—The intriguing problem of classifying finite subsets S of points in the Euclidean plane such that no three points in S are collinear and such that the distance between any two points in S is rational, is discussed in **[K1]**$'$. The problem has a curiously "Diophantine ring" to it but one doesn't immediately see how to put it into a familiar category. Apparently, the case where S has cardinality 4 has been attacked by Brahmegupta, Kummer, and Mordell **[Kl, Mo 2]**$'$.

(d) [Representing integers, or rational numbers, by some given polynomial] Any positive integer is a sum of four squares. The number of ways in which a natural number n can be expressed as a sum of k squares (or, more generally, can be represented by a given positive-definite quadratic form) yields a fascinating array of arithmetic functions of n, and a profound understanding

[3] Not to leave the reader with the impression that the "smallest solution" is always as small as our example above, let us cite the case $X^2 - 109 \cdot Y^2 = 1$ whose smallest solution is

$$(158071986249, 15140424455100),$$

as was known to Fermat (cf. discussion on p. 97 of **[Wl]**$'$).

[4] See Koblitz's book **[Ko]**$'$, which is devoted to this problem.

[5] *Answer*: Not if the *genus* is greater than one! This is essentially equivalent to Mordell's conjecture, recently proved by Faltings—the focus of these talks.

of these functions[6] is one of the impressive achievements of classical number theory.

I don't mean to say that we now fully understand these matters. Far from it: the richness of structure of these arithmetic functions has been a source of amazement to everyone who has encountered them, and their connections with some of the other great problems in mathematics[7] are labyrinthine.

There is also no dearth of problems involving polynomials of higher degree (Waring's problem being, perhaps, the most well known). Here are two problems (in "few variables") where in each case an affirmative answer would settle an important long-standing issue in the arithmetic of elliptic curves:

(Silverman's problem.) *For any natural number k, is there a* ***cube-free*** *integer that can be represented as a sum of two cubes in at least k ways?*

Readers of Hardy's account of Ramanujan's last days will remember the taxicab license that settles this for $k = 2$.

(Weil's "1929 problem" [W1929]′.) *Is there a general algorithm to settle the question of whether or not a fourth-degree polynomial with rational coefficients in one variable represents the square of a rational number?*

(For any fixed number field one would also want a corresponding algorithm.)

2. Systematic formulations. One does not have to wait long, in the history of the development of algebra to hear calls for the systematic treatment of the problems at issue. The modern inventor of algebra (François Viète) ends his treatise *Introduction to the analytic art*, which is dedicated to a contemporary [~ 1591] descendant of the "fairy Melusine", [**Vi 1, 2**]′ with the bold:

> *Finally the analytical art, having at last been put into the threefold form of zetetic, poristic, and exegetic, appropriates itself by right to the proud problem of problems, which is*
>
> **TO LEAVE NO PROBLEM UNSOLVED.**[8]

A clearer formulation of this sentiment is given by Hilbert [**Hi**]′ in his 10th problem.

Determination of the solvability
of a Diophantine equation

> *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 solvable in rational integers.***

Readers are probably aware that some 15 years ago, Matijasevic showed that

[6] They also arise as Fourier coefficients of classical, and not-so-classical, modular forms.

[7] For example, sphere-packing problems (of course), the structure of the Monster group, the representation theory of the group of automorphisms of the algebraic closure of the field of rational numbers, the infinite-dimensional representation theory of some linear algebraic groups (like $\mathbf{GL}_2$), to say nothing of a myriad of other (at first view unrelated) important Diophantine problems.

[8] "fastuosum problema problematum ars Analytice... iure sibi adrogat, Quod est, NULLUM NON PROBLEMA SOLVERE" (the capital letters are Viète's).

no such process as envisaged by Hilbert exists, at least if by process one means computing machine algorithm. An ironical element in Matijasevic's proof is that the very success that we have in enumerating *all* solutions of a Pellian equation [e.g., our example §1(b) would suffice for his purposes; cf. **[D-M-R]**′] is used as a lever to demonstrate the nonexistence of general algorithms.

It is still unknown, however, whether or not there are general algorithms to determine whether equations are solvable in rational *numbers* (rather than rational integers).[9]

Now a few words about Diophantine questions, organized by degrees:

Degree 1

Even here, where Cramer's rule completely takes care of the question of rational solutions, if one asks for the "smallest" integral solutions of a system of linear equations with integral coefficients in many variables, one finds one's self in difficult terrain, within the realm of the "geometry of numbers". Good asymptotic bounds are of considerable importance, for example, for the production of "auxiliary polynomials" to be used in the theory of transcendental numbers. See **[B-V]** for the latest and best bounds.

Degree 2

Homogeneous forms of degree two (quadratic forms) have the agreeable property that if you are given one nontrivial rational solution, you can get the rest by a systematic procedure. We shall see this later in a special case (the "method of sweeping lines").

Definite quadratic forms have no nontrivial real solutions, and hence no rational ones. Indefinite quadratic forms with rational coefficients in 5 variables or more always have a nontrivial rational zero. There are, in general, effective procedures to determine whether or not a quadratic form has a rational zero.

As mentioned above, the question of representing *integers* by quadratic forms is vast, and seems at present open-ended.[10] So is the question of

[9] In view of higher-dimensional Mordell conjectures of Lang **[L 5]**, Bombieri and Vojta, it is tempting to pose some "effectivity problems" which are more pliable than the classical ones described in the text. For example, say that a polynomial equation $f(X_1, \dots, X_N) = 0$ is *arithmetically dense* if there exists a number field K such that the K-solutions of f [i.e., $(a_1, \dots, a_N) \in K^N$ such that $f(a_1, \dots, a_N) = 0$] are so numerous that any polynomial $\varphi(X_1, \dots, X_N)$ vanishing on all K-solutions, vanishes on all $\mathbb{C}$-solutions as well. Is there an effective algorithm to determine whether a given polynomial f is arithmetically dense?

A technical note concerning arithmetic density:

The notion of arithmetic density may be framed in the more general context of algebraic varieties. By Faltings' theorem, and known simple results, a curve is arithmetically dense if and only if its genus is $\leqslant 1$. As for varieties of arbitrary dimension, see an account of specific conjectures and results in this area in a forthcoming survey article by Lang. One has, for example, a conjecture due to Bombieri and Lang that arithmetically dense varieties are not of general type. One also has partial confirmation of this conjecture in the context of function fields (see **[No]**; see also the earlier related work of Bogomolov, e.g. **[Des]**).

It seems fair to say, however, that at the present moment we lack sufficient experience to make definitive conjectures concerning arithmetic density, covering all varieties, or even covering all surfaces. Are there, for example, $K3$ surfaces which are not arithmetically dense?

[10] It was only relatively recently proved by Siegel (1972) that this problem is effective. Other effective proofs have been given subsequently by Cassels **[Ca]**′ and Benham-Hsia **[B-H]**.

classifying quadratic forms up to integral General Linear change of variables.[11] (The case of two variables alone, a study initiated by Fermat, Euler, Lagrange, and especially Gauss—in modern terms: "the ideal class group of quadratic number fields"—still presents innumerable mysteries.)

Degree 3

There are at present, no proved algorithms to determine whether a general homogeneous form in three variables with rational coefficients has a nontrivial solution (we will discuss this case at much greater length later). A theorem of Heath-Brown proved in this past year guarantees, however, that any smooth (nonsingular) such form in 10 variables or more does have a nontrivial rational solution. This improves upon prior results of Davenport and Birch; it is also "best possible" in the sense that there are such forms in 9 variables without nontrivial solutions. In contrast to the case of degree 2, finding *one* nontrivial rational solution does not end the matter: the fun only then begins, as we shall see later in the case of three variables.

The theory of integral representations is in an incomparably more primitive state than for degree 2. It has been known for a long time, for example, that any natural number is representable by 9 (or fewer) perfect cubes, 9 being best possible, but we are in the dark about more refined questions (i.e., Silverman's problem described above).

As for classification, there are the beginnings of a fascinating theory of binary (i.e., two-variable) cubic forms, initiated by Davenport, Heilbronn, and Shintani.

Degree $\geqslant 4$

Following the work of Matijasevic, J. P. Jones has produced a polynomial, $f_a(x_1,\dots,x_{153}) = f(a;\ x_1,\dots,x_{153})$, of degree 4 in 154 variables such that the question of whether or not, for a given integral value of the parameter a, f_a has a *positive integer zero* can never be settled by a computing machine algorithm.

As for rational solutions, although a theorem of Birch guarantees that for any odd degree d, there is a number $N(d)$ such that a homogeneous form of degree d in N variables with rational coefficients ($N \geqslant N(d)$) has a nontrivial rational solution, one still doesn't have a good guess for the best $N(d)$. Nor are there algorithms (even in cases as special as Weil's "1929 problem" above).

For the rest of these lectures—after a digression on the question of integral solutions and their connections with Diophantine approximation—we shall concentrate on the problem of rational points on curves.

3. Digression: Questions of integral solutions vs. Questions of Diophantine approximations. Let us return to the fact, discussed in §1(b), that there are an infinity of rational approximants x/y to $\sqrt{2}$ satisfying the inequality

$$|x/y - \sqrt{2}| \leqslant c/y^2.$$

The celebrated theorem of *Roth* underscores the fact that this infinity of approximants has just barely "squeaked through". That is, Roth's theorem

[11] Or the more general question of representing one quadratic form by another.

asserts that for α any algebraic irrationality and for (c, ε) any choice of positive constants, *there are only a finite number of approximants x/y to α* satisfying the inequality

$$|x/y - \alpha| \leqslant c/y^{2+\varepsilon}.$$

A major drawback in our understanding of Roth's theorem is that the method of proof provides no effective way of determining the finite set of approximants in question.[12] This drawback casts its shadow on all of the applications of Roth's theorem to questions concerning integral solutions, as we shall soon see.

Perhaps the quickest way to see that Roth's theorem says something important about integral solutions is to consider a particular equation, like

$$X^3 - 7 \cdot Y^3 = m$$

for some fixed integer m. The main requirement of the particular equation we choose is that, in contrast to the Pellian equation, its degree is > 2. By reasoning utterly analogous to that of §1(b) we may obtain a constant c (which depends upon the choice of m) such that if (X, Y) is an integral solution to our equation, then

$$|X/Y - \sqrt{7}| \leqslant c/Y^3.$$

But, choosing ε so that $2 + \varepsilon < 3$, Roth's theorem immediately implies that there are at most a finite number of such approximants, from which one deduces that our equation admits at most a finite number of integral solutions. By more elaborate arguments, but ultimately appealing to the same Roth's theorem[13] Siegel proved the following general result:

THEOREM (SIEGEL). *Let $f(X, Y)$ be an irreducible polynomial with integral coefficients. Then the equation $f(X, Y) = 0$ has only a finite number of integral solutions (X, Y) except in the following special case*:

(a) *The curve $f(X, Y) = 0$ can be rationally parametrized, i.e., there are rational functions $X(t)$, $Y(t)$ of a variable t, not both constant, such that $f(X(t), Y(t))$ vanishes identically, and*

(b) *the projectivized curve (see Part* II *below) has at most two points at ∞.*

By virtue of the fact that Siegel makes use of Roth's theorem in his proof, no effective way is given to find the finite number of integral solutions of the equations $f(X, Y) = 0$ covered by the theorem. There is an alternative method, due to Baker, which establishes the finitude of the number of integral solutions of a class of equations of the form $f(X, Y) = 0$. Baker's method is based on an effective estimate for a lower bound satisfied by linear forms in logarithms, rather than on Roth's theorem. Its disadvantage vis a vis Siegel's theorem is that Baker's method covers only a restricted class of such equations. It would, in fact, be interesting to have a satisfying explanation as to why Baker's

[12] The number of approximants can, however, be bounded [**D-R**].

[13] In fact, Siegel's theorem (1929) pre-dated the discovery of Roth's theorem (1955). Siegel was constrained to appeal to a weaker result, antecedent to Roth's theorem (his own sharpening of a theorem proved in 1909 by Thue) and had to resort to concomitantly more elaborate arguments.

method is inapplicable more generally, and, perhaps, to have a conceptual description for its precise domain of applicability. The great advantage of Baker's method is that, when it is applicable, it provides an effective result.[14]

An example of an equation for which both Baker's method and (of course) Siegel's theorem applies is:

$$AY^2 + BX^3 = M$$

for fixed integer nonzero constants A, B and M. Such equations have been the focus of much study for various reasons: First, the nature (e.g. finiteness) of their solutions visibly bears upon the phenomenology of the placement of the set of "perfect squares" and "perfect cubes" in integers. Second, such equations arise as rather natural "next-most-simple cases" to contrast to the Pellian equations which exhibit vastly different behavior. But perhaps the most important reason to consider them in detail is that (for certain A, B) their solution plays a critical role in classifying certain structures of Diophantine importance. We shall touch upon this below, and in anticipation of the role that these equations play, we call them: *generalized cubic discriminant equations.*

Applying Baker's method, Stark established the following "almost exponential" upper bound for the size of solutions to generalized cubic discriminant equations:

For fixed A, B, and for every $\varepsilon > 0$, there is a constant $c = c(\varepsilon)$ such that if (X, Y) is an integral solution of $AY^2 + BX^3 = M$, then

$$|X| < c^{|M|^{1+\varepsilon}}.$$

However powerful the above estimate may be, it is likely to be quite far from the actual phenomena. Specifically, M. Hall has conjectured:

(?) *For fixed A, B and for every $\varepsilon > 0$, there is a constant $C = C(\varepsilon, A, B)$ such that if (X, Y) is an integral solution of $AY^2 + BX^3 = M$, then*

$$|X| < C \cdot |M|^{2+\varepsilon}.$$[15]

We now devote ourselves to the study of rational points.

II. CURVES

1. Plane curves. Let K be a subfield of $\mathbf{C}$, the field of complex numbers. The most important examples for us are $K = \mathbf{Q}$, the field of rational numbers, and $K = \mathbf{C}$. We shall be dealing with polynomial equations in two variables with coefficients in K, $\varphi(x, y) = 0$. As a running example, let us take the *Klein curve* (Figure 1).

If one's aim is to study *K-rational solutions*, i.e., points (a, b) in the "finite plane" $K \times K$ such that $\varphi(a, b) = 0$, one loses little and often gains some simplicity by passing to the projective plane. This is a truth universally acknowledged since the days of Poncelet, but notice that if we were interested

[14] But, the bounds provided are usually enormous.

[15] See [**Hall**] for computer evidence for this conjecture. See [**Si**] and [**Ma**] for its treatment and the treatment of analogous problems in the context of function fields. See [**Vo**] for the role that Hall's conjecture plays within the realm of more general conjectures of Vojta.

in the question of *integral* solutions, we could not "projectivize". To pass to the projective plane amounts to replacing the polynomial $\varphi(x, y)$ by its associated homogeneous form $f(u, v, w)$. The associated form $f(u, v, w)$ is characterized by the requirements that it be homogeneous, of the same degree as φ, and such that $f(x, y, 1) = \varphi(x, y)$. In the case of the Klein curve, the homogeneous form is

$$f(u, v, w) = u^3v + v^3w + w^3u. \tag{1}$$

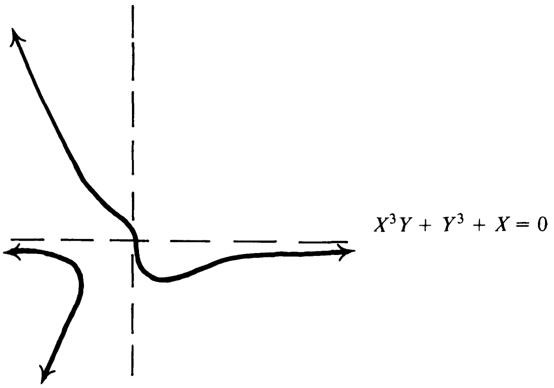


FIGURE 1

Digression about real points. In the above picture, the real locus of the Klein curve is seen to have two connected components in the finite plane. They "hook together" to make a single component in the projective plane. The number of components of the real locus of an algebraic curve, and their placement (possible nesting configurations) has been a topic of continued concern, and the problem of Hilbert devoted to this (the 16th problem) is far from settled. About a century ago, Harnack proved that a smooth real algebraic curve of degree d can have a maximum of

$$(d - 1)(d - 2)/2 + 1$$

components and that for every degree this maximum is realized.

I can't resist reproducing A'Campo's beautiful, intriguing picture of a real algebraic curve of degree 6 with the maximum number of components a curve of its degree can have (Figure 2). This appears in his account of recent progress towards Hilbert's 16th problem [A].

Recall that the *K-rational points* of the projective plane are equivalence classes of triples (a, b, c) in $K \times K \times K$ such that a, b, and c are not all zero, and where the equivalence relation is given by scalar multiplication by nonzero elements in K. As usual, we denote by $\mathbb{P}^2(K)$ the set of K-rational points in the projective plane.

We shall reserve the term *plane curve* to refer to a curve C in the projective plane given by an equation:

$$f(u, v, w) = 0 \tag{2}$$

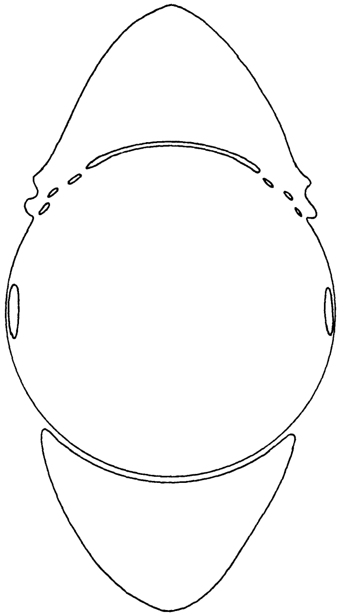


FIGURE 2 (Reprinted, with permission, from Norbert A'Campo, Sur la première partie du seizième problème de Hilbert (Séminaire Bourbaki, exp. 537, Juin 1979), Lecture Notes in Mathematics, vol. 770, Springer-Verlag, 1980, p. 216)

where f is a homogeneous *irreducible* form. The *degree* of C is the degree of the form f.

Two homogeneous forms which are nonzero scalar multiples of one another define the same curve. A curve C is *defined over* K if there is a homogeneous form f defining C, all of whose coefficients lie in K. Equivalently, given any homogeneous form f defining C, C is *defined over* K if the ratio of any two nonzero coefficients of f lie in K. Our Klein curve, for example, is defined over $\mathbf{Q}$.

If the plane curve C is defined over K, then the set of K-rational points on the curve C, denoted $C(K)$, is the set of K-rational points in the projective plane which are solutions of (2); that is, a K-rational point on C is an equivalence class of triples (a, b, c) in $K \times K \times K$ such that $f(a, b, c) = 0$, the equivalence relation being given by scalar multiplication by nonzero elements of K. The question of determining $C(K)$, even in specific instances, is notoriously difficult. If you wish to convince yourself of the difficulty of this problem, try to find all $\mathbf{Q}$-rational points on our Klein curve! For the answer, see [**Hu**].

2. Algebraic curves. Why not consider, more generally, algebraic curves in projective space of any dimension N? We certainly can do so, and, moreover, all the work we are about to discuss will make reference, in essence, only to the *intrinsic* algebraic geometry of curves. No use will really be made of the way the curve sits in projective space. Nevertheless, if you want to keep some "concrete model" in mind, there is little harm in sticking to plane curves, when studying K-rational points. This is because any algebraic curve X in projective N-space may be linearly projected in a generically one:one way into the projective plane. There are, in fact, many such linear projections, and if X is defined over K, such linear projections may be found which are also defined over K. The image of X under such a projection (generically one:one on X and defined over K) is a plane curve C defined over K, and (a matter of great importance for us), the K-rational points of X and of C are closely related.[16]

3. Smooth curves. Recall that the *singular* or *nonsmooth* points of a plane curve are those points on the curve at which all the partial derivatives

$$\frac{\partial f}{\partial x}, \quad \frac{\partial f}{\partial y}, \quad \frac{\partial f}{\partial z}$$

vanish. Our Klein curve, for instance, is smooth, since there are no simultaneous solutions of

$$f = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = \frac{\partial f}{\partial z} = 0$$

for f as in (1).

Any algebraic curve C in projective space is the (generically one:one) linear projection of a smooth algebraic curve X in some higher-dimensional projective space. Such a curve X is called a *smooth model* for C.

If C is defined over K, it possesses a smooth model X defined over K such that the linear projection bringing X to C is also defined over K. It will usually be to our advantage to replace any curve C by its smooth model X as soon as possible. We will also reserve the letter X to denote smooth algebraic curves.

4. Riemann surfaces. If X is a smooth algebraic curve, its $\mathbf{C}$-rational points $X(\mathbf{C})$, viewed as imbedded in complex projective N-space, cuts out a compact Riemann surface. Conversely, if Z is any compact Riemann surface, Z is analytically isomorphic to the complex locus of an algebraic curve in projective space. This well-known, yet ever-mysterious connection between complex analysis and algebraic geometry is a very stringent "link" indeed: Given, for example, any Riemann surface analytically imbedded in projective N-space, one may view it as the locus of common complex zeroes of a finite number of homogeneous polynomial forms $(f_j = 0)_j$ and hence as the Riemann surface associated to an algebraic curve X. This phenomenon is the simplest instance of *Chow's theorem*, which will serve us well, in its greater generality, later on. This "link" persists in the context of mappings between Riemann surfaces as well. If X and Y are two algebraic curves and $f\colon X(\mathbf{C}) \to Y(\mathbf{C})$ an analytic mapping between their Riemann surfaces, then f "is" algebraic

[16] Questions pertaining to *integral* points, sometimes suffer much greater injury under such generically one:one projections.

in the sense that its graph, imbedded in $X(\mathbb{C}) \times Y(\mathbb{C})$, and then in projective $MN + M + N + 1$-space:

$$\operatorname{graph}(f) \subset X(\mathbb{C}) \times Y(\mathbb{C}) \subset \mathbb{P}^N(\mathbb{C}) \times \mathbb{P}^M(\mathbb{C}) \subset \mathbb{P}^{MN+M+N}(\mathbb{C})$$

"Segre imbedding"

is the locus of complex points of an algebraic curve Γ.

Given X, Y two algebraic curves defined over K, a *mapping* f: $X \to Y$ *defined over* K will mean a mapping between their Riemann surfaces such that the algebraic curve Γ is defined over K. It is important to notice that this concept of mapping is *intrinsic* to X, and in an essential sense it ignores the placement of X in projective space. Armed with this concept, we can of course define *isomorphism between two algebraic curves defined over* K.

The smooth model of an algebraic curve defined over K is unique, up to isomorphism defined over K.

5. Simplifying the singularities of a plane curve:

If C is a plane curve and X is its smooth model in some high-dimensional projective space, the image of X under a generic projection to a 2-dimensional projective space yields another plane curve C' with at worst *nodal* (or *ordinary double point*) singularities. These are singularities which look (analytically) like $X \cdot Y = 0$.

EXAMPLE. The diagram (Figure 3) is a picture of a degree 5 plane curve with four singularities (all nodes).

As we shall see below, it has genus 2.

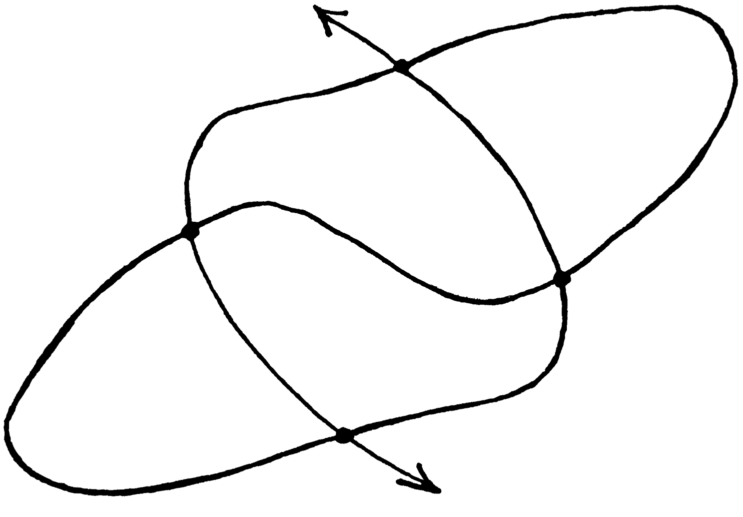


FIGURE 3

Since C and C' share the same smooth model X (all defined over any field K over which C is defined) questions about K-rational points of C and C' are closely related. So, again, one hardly loses any generality by restricting attention to plane curves C with only nodal singularities. For these curves passing from C to the smooth model X is easily envisaged: One simply separates the two sheets of each of the ordinary double points (see Figure 4).

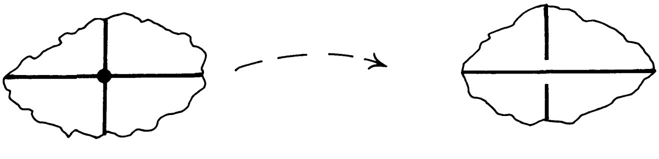


FIGURE 4

6. Genus. If X is a smooth algebraic curve, the *genus* g_X may be defined to be the "number of handles" of the Riemann surface $X(\mathbf{C})$. For example, in Figure 5, $g_X = 5$.

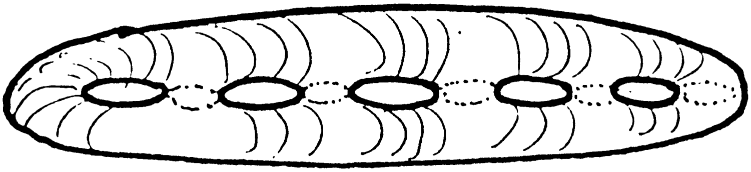


FIGURE 5

More precisely, g_X can be defined *topologically* by the formulae

$$g_X := 1 - \chi/2 = b_1/2,$$

where χ is the Euler characteristic and b_1 is the first Betti number of the topological 2-manifold $X(\mathbf{C})$.

The genus can also be defined *analytically* as the number of independent analytic differential 1-forms on the Riemann surface $X(\mathbf{C})$. If X is defined over K, it is also the number of K-linearly independent regular (algebraic) differential 1-forms defined over K.

If C is a plane curve with only nodal singularities, then g_X, the genus of a smooth model X, is given by the formula:

$$g_X = \frac{(d-1)\cdot(d-2)}{2} - \nu, \tag{3}$$

where d is the degree of C and ν is the number of (nodal) singular points.

EXAMPLES. This formula shows that smooth plane curves are a rarity, and that singularities on plane curves can be an unavoidable annoyance. For example, any plane curve whose smooth model is of genus two[17] must have at least one singular point. Any smooth curve of genus two may be found in $\mathbf{P}^3$, however, as an irreducible component of the intersection of a cubic and a quadric.

[17] Or, more generally, whose genus is not a "triangular number".

As the genus grows, very little is known about the smallest degree that a (birational) plane curve model for a given algebraic curve may have. For the "general curve" of genus g, the smallest degree is $[(2g + 8)/3]$ and hence it will not fail to have singular points (if they are all nodal, then the number is asymptotic to $2g^2/9$). See the discussion of this in Lecture 1 of [**Mu**]′.

For the Klein curve, $d = 4$, $\nu = 0$, so it is of genus 3.

7. The fundamental trichotomy. Let X be a smooth algebraic curve defined over K. The "trichotomy" to which I am referring is: the genus of X equals *zero*, *one* or is *greater than or equal to* 2.

Genus zero

Analytic structure. The associated Riemann surface $X(\mathbb{C})$ is isomorphic to the Riemann sphere. It is a homogeneous space under the action of its automorphism group $\mathbf{PGL}_2(\mathbb{C})$.

Differential geometry. The Riemann surface $X(\mathbb{C})$ carries a Riemannian metric of constant positive curvature.

K-rational points. If X possesses a K-rational point, then X is isomorphic over K to the projective line $\mathbb{P}^1$. In this case $X(K)$ is rationally parametrized by (and is in one:one correspondence with) $\mathbb{P}^1(K)$.

Summary. $X(K)$ is either empty or of infinite cardinality. If K is the field of rational numbers, or more generally a number field, then one can effectively determine which of the two possibilities occurs.

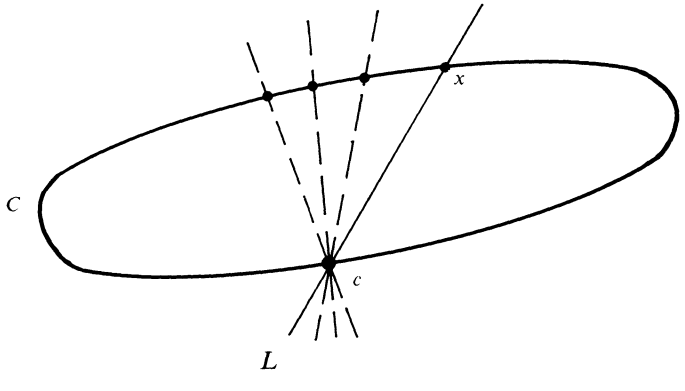


FIGURE 6

EXAMPLES. Take C to be defined by any irreducible conic in the projective plane, with a K-rational point c on it. Let us realize $\mathbb{P}^1(K)$ as the set of (K-rational) lines in the projective plane passing through c. Every such line L will intersect C in a unique point x "other than" c [if L is tangent to C at c, we take x to be equal to c]. The association $L \mapsto x$ is the parametrization of $C(K)$ by $\mathbb{P}^1(K)$ (the method of *sweeping lines*).

For instance, we might take the famous conic $X^2 + Y^2 - Z^2 = 0$ which expresses the problem of parametrizing *Pythagorean triples*.

Another example would be given by any irreducible cubic C with a singular point c. Such a singular point is necessarily unique, and is defined over any field K over which C is defined. The genus formula (3) then gives that g_X, the genus of a smooth model of C, is zero. Using the method of "sweeping lines" based at the singular point c, one again gets a rational parametrization of the points of C.

Genus one

Analytic structure. The Riemann surface $X(\mathbf{C})$ is isomorphic to a *complex torus of dimension one*. Let us take some time out to recall what a complex torus (of any dimension) looks like.

A *lattice* Ω in $\mathbf{C}^n$ (complex n-space) is a discrete subgroup which generates $\mathbf{C}^n$ as a real vector space; or, alternatively, it is a discrete subgroup which is a free abelian group on $2n$ generators. For example, the *hexagonal lattice* in the complex plane (Figure 7).

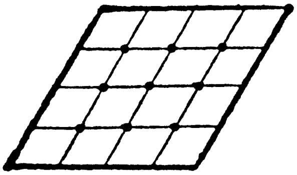


FIGURE 7

A *complex torus of dimension n* is a complex analytic Lie group isomorphic to the quotient of $\mathbf{C}^n$ by a lattice Ω.

For example, if $n = 1$, we are taking the quotient of the complex plane by a lattice (by "two periods") and we obtain a torus in the old-fashioned sense, e.g., for the hexagonal lattice we get the Riemann surface obtained by pasting (Figure 8) and this Riemann surface comes with a natural (analytic) group law on it.

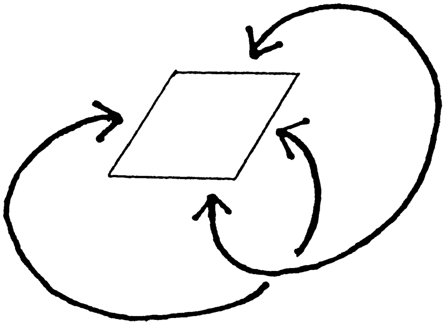


FIGURE 8

An essential property of complex tori is that their group structure is determinable purely from their complex analytic structure, at least if you provide your complex torus with a "basepoint" to act as the origin for the group law. Specifically, suppose

$$T_1 = \mathbf{C}^{n_1}/\Omega_1, \qquad T_2 = \mathbf{C}^{n_2}/\Omega_2$$

are complex tori, and t_i in T_i are the image of the origin in each. Then any complex analytic mapping from T_1 to T_2 which brings t_1 to t_2 is induced from a *complex linear* mapping from $\mathbf{C}^{n_1}$ to $\mathbf{C}^{n_2}$.

Differential geometry. Any complex torus (of any dimension) carries a flat metric induced from complex n-space, hence so does $X(\mathbf{C})$.

K-rational points. As in the case of genus zero, it may happen that $X(K)$ is empty. If not, choose a K-rational point x_0, and give $X(\mathbf{C})$ its canonical group structure with x_0 as origin. It then follows that $X(K)$ is closed under the addition law, and so can be considered as a (commutative) group in its own right. The theorem of *Mordell-Weil* asserts that if K is the rational field, or, more generally, a number field, then $X(K)$ is finitely generated. That is,

$$X(K) \cong \mathbf{Z}^r \oplus [\text{finite abelian group}].$$

REMARK. When K is the rational field $\mathbf{Q}$ it is known that only *fifteen* finite abelian groups can occur as torsion subgroups of $X(\mathbf{Q})$ for some X, and each of these fifteen groups do occur infinitely often. Far less is known about the mysterious number r, and at present we still do not have a (proved) algorithm for computing r. Nor do we have an algorithm (established, independent of any conjectures) to determine whether a curve X of genus 1 has *any* rational K-rational solution points. If we could determine this latter question effectively, then we could compute r effectively. John Tate brought to my attention the article **[W 1929]** of Weil, published in 1929, where he showed that an effective algorithm to determine whether any given quartic in one variable with coefficients in K represents a square in K (Weil's "1929" problem I.2) would yield an effective solution to both questions discussed above. As for the possible values of r, it is generally expected that there are curves of genus 1 over $\mathbf{Q}$ with arbitrarily large r, but this hasn't yet been shown. It is known that an affirmative answer to "Silverman's problem" (I. §2) would substantiate this. At present, an example due to Mestre (obtained via a quite interesting method) has r at least equal to 14 (see **[Me 1]** for $r \geqslant 12$; **[Me 2]** for $r \geqslant 14$).

EXAMPLES. Let $\varphi(x, y) = y^2 - g(x)$ where $g(x)$ is a cubic polynomial in x with distinct roots, and let C denote the plane cubic defined by the homogeneous form associated to φ. Then C is smooth, i.e., we may take $X = C$, and C has a unique point at infinity. Take x_0 to be this point at infinity. Since C is a cubic, any line in the projective plane intersects C in three points (counted with multiplicity).

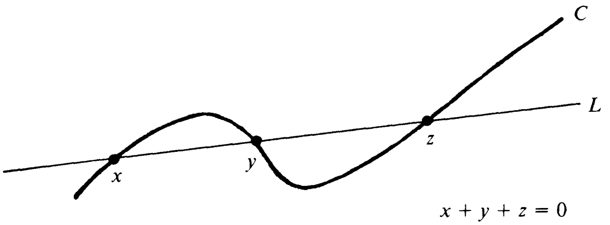


FIGURE 9

The group law on $X(\mathbb{C})$ is characterized by the property that the *sum* of any three collinear points is equal to zero, i.e., to x_0.

This beautiful, geometrically defined, group law on smooth cubics has often been referred to as the *chord-and-tangent method*, because in a concrete sense it may be thought of as a way of generating new K-rational points from old: Given two K-rational points x and y, draw the line L through x and y (viewed as a "chord" on C). Then L will intersect in a unique third point z on C (necessarily K-rational again). Of course if you take $x = y$, then L should be taken to be the tangent to C at x. In these terms, the Mordell-Weil theorem then guarantees that there is a *finite* set of K-rational points, if K is a number field, such that any other K-rational point can be obtained by assiduous iterated application of the "chord-and-tangent method" starting with this finite set.

SUBEXAMPLE 1. An integral solution to

$$y^2 + y = x^3 - x$$

provides an example of a product of two consecutive integers being equal to a product of three consecutive ones.

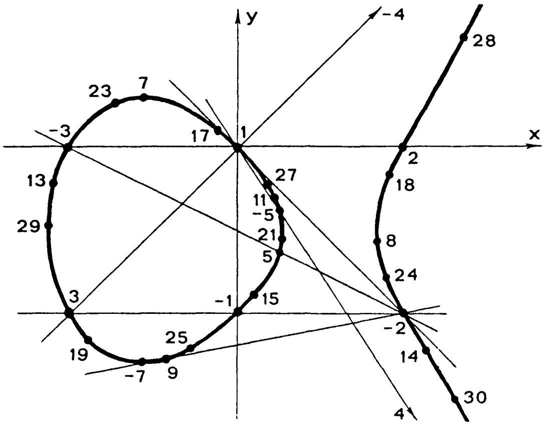


FIGURE 10. Rational points on the curve $y^2 + y = x^3 - x$. (Reprinted, with permission, from Algebraic Geometry, by Robin Hartshorne, Springer-Verlag, 1977, p. 336. Artist: Richard Bassein.)

Consider the plane cubic C which is the projectivized form of the above curve. Then C is smooth, i.e., we can take X equal to C, giving it a group structure with the unique point at infinity as origin. Clearly, $(x, y) = (0, 0)$ is a nontrivial point, call it P, in $X(\mathbb{Q})$. It can be shown that $X(\mathbb{Q})$ is free on the single generator P. An elementary exercise gives that if (a, b) are the coordinates of a point R on X, and a is nonzero, then the coordinates (a', b') of $R + P$ are given by

$$a' = \frac{b^2 - a^3}{a^2}; \qquad b' = 1 - \frac{b}{a}a'.$$

Here is a list of the absolute values of the numerators of the X-coordinates of various multiples $m \cdot P$ (m running through even integers between 8 and 58).

20
116
3741
8385
239785
59997896
1849037896
270896443865
16683000076735
2786836257692691
3148929681285740316
342115756927607927420
280251129922563291422645
804287518035141565236193151
743043134297049053529252783151
3239336802390544740129153150480400
2613390252458014344369424012613679600
12518737094671239826683031943583152550351
596929565407758846078157850477988229836340351
2385858586329829631608077553938139264431352010155
56186054018434753527022752382280291882048809582857380
2389750519110914018630990937660635435269956452770356625916
65008789078766455275600750711306493793995920750429546912218291
8633815035886806713921361263456572740784038065917674315913775417535
43276783438948886312588030404441444313405755534366254416432880924019065
593076045469642658948956761739794324482729234687114512318727773285876671389

SUBEXAMPLE 2. Curves of genus one also arise as the locus of intersection of two smoothly intersecting quadrics in projective three-space. For example, consider the projectivized curve obtained from the pair of equations:

$$X^2 - N = Y^2; \qquad X^2 + N = Z^2,$$

where N is a nonzero rational number. A (simultaneous) rational solution to the above pair of equations answers the problem of finding a rational square ($r = X^2$) which augmented or diminished by N remains a rational square. I am thankful to D. Zagier for providing me with the example of $N = 157$ where the "simplest" rational square $r = X^2$ which answers the problem is:

$$\frac{50356938758080675904478428415148993121355253942510969278703974330010718396658421418332558705681}{317718665887162537529860429204893522122457849878951860106775096212089198787035991271029955600}.$$

Here, "simplest" means smallest numerator and denominator.

For more examples of curves of genus one with small coefficients yet whose simplest solution is impressively large, see [**B-C**].

EXERCISE. Find an analogue of the "chord-and-tangent method" valid for plane quartics possessing precisely two (nodal) singularities. To do this, define a *special point* on such a plane curve to be a point x_0 for which there exists a conic passing through the two singular points and having order of contact 4 with C at x_0. Now fix such a special point x_0 and replace the use of lines in the chord-and-tangent method by conics passing through x_0 and the two nodes.

Genus $\geqslant 2$

Analytic structure. The universal covering space of the Riemann surface $X(\mathbf{C})$ is isomorphic to the Poincaré disc. The group of analytic automorphisms of $X(\mathbf{C})$ is finite. Its order is $\leqslant 84(g-1)$ where g is the genus of X.

Differential geometry. The Riemann surface $X(\mathbf{C})$ carries a hyperbolic metric, i.e., a Riemannian metric of constant negative curvature.

K-rational points. Let K be the field of rational numbers, or more generally any number field. Then

THEOREM OF FALTINGS (MORDELL'S CONJECTURE). *$X(K)$ is finite.*

REMARKS. The above theorem is, at present, ineffective: We lack a finite algorithm to determine whether or not a given curve X possesses a K-rational point. It is very likely, however, that we shall have in the near future a computable upper bound for the cardinality of $X(K)$. (Consult **[F-W]**$'$ and **[Szp 2]**$'$.) But since the computable upper bound provided by general arguments is surely much larger than the actual number of rational points (in any case of interest) this bound may not be much help in the project finding all rational points in any instance. In this connection one might mention some recent results of Coleman who has obtained extremely good upper estimates for the *number* of K-rational points on curves in very special cases, by developing a sharp effective version of an old result of Chabauty **[Co]**.

We also lack significant numerical data (the principal reason being that this data is hard to gather). For example, for a given number field K (e.g., the rational field) and for a given $g \geqslant 2$, are there curves X of genus g defined over K with arbitrarily large $X(K)$? (presumably yes). Or, fixing X, how does the size of $X(K)$ vary as K ranges though some specified (infinite) set of number fields?

Before Faltings proved his theorem, for *no* curve X of genus $\geqslant 2$ was it known that $X(K)$ is finite for all number fields K.

EXAMPLE. Consider the Klein curve again (1)

$$C\colon\ u^3v + v^3w + w^3u = 0.$$

Recall that C is smooth of genus 3. The automorphism group is isomorphic to $\mathbf{PSL}_2(\mathbb{F}_7)$, the simple group of order 168, which is the largest order possible for the automorphism group of a Riemann surface of genus 3.[18] By Faltings' theorem, $C(K)$ is finite for any given number field K.

There are many ways of seeing why the group of automorphisms of a compact Riemann surface of genus $\geqslant 2$ is finite. As John Hubbard said: the points on such a Riemann surface have a "rugged individuality"—there are a myriad of finite subsets of points, each subset defined by distinct special (analytic) properties, e.g., Weierstrass points, and their generalizations, and any symmetry of the Riemann surface must preserve all this structure. We shall prove a stronger result (de Franchis' theorem) which implies finiteness of the group of symmetries. de Franchis' theorem is used in Faltings' proof of

[18] The 168 automorphisms are rational over the field $\mathbf{Q}(\zeta)$ where ζ is a primitive 7th root of 1. An automorphism of order 7 is given by $u \mapsto \zeta u$, $v \mapsto \zeta^4 v$, $w \mapsto \zeta^2 w$.

Mordell's conjecture, and it also can be regarded as a special case of the geometric analogue of Mordell's conjecture (see §9), so it may be worth dwelling on.

8. Interlude: geometric finiteness results.[19]

THEOREM OF DE FRANCHIS. *Let Y and Z be closed Riemann surfaces, with Z of genus $g_Z \geqslant 2$. Then there are only a finite number of nonconstant analytic mappings from Y to Z.*

There is also the more encompassing finiteness result:

THEOREM OF DE FRANCHIS-SEVERI. *Let Y be a closed Riemann surface. Then there are only a finite number of mappings $f\colon Y \to Z$ (taken up to isomorphism) where Z ranges through all closed Riemann surfaces of genus $\geqslant 2$ and f ranges through nonconstant (holomorphic) mappings.*

Both of the above results give effective upper bounds.

a. The theorem of de Franchis. A common ingredient to all proofs of the theorem of de Franchis is the idea of replacing analytic mappings from Y to Z by their graphs $\Gamma \subset Y \times Z$ (Figure 11).

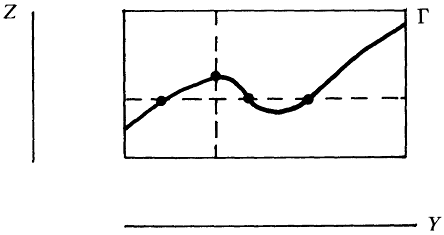


FIGURE 11

The curve Γ is isomorphic to Y via the projection to first coordinate. We must show that the number of curves on the surface $Y \times Z$ which can be the graphs of nonconstant mappings from Y to Z, is finite.

Attached to any such curve Γ on $Y \times Z$ is its fundamental (cohomology) class $c(\Gamma) \in H^2(Y \times Z; \mathbb{Z})$. We have the following restrictions on the class $c(\Gamma)$. If $\cdot$ denotes intersection number, then (since Γ is a graph of a function)

$$c(\Gamma) \cdot \text{pt.} \times Z = 1 \tag{3.a}$$

and, if $d = \text{degree}(f)$,

$$c(\Gamma) \cdot Y \times \text{pt.} = d. \tag{3.b}$$

We also have that

$$c(\Gamma) \cdot c(\Gamma) = d(2 - 2g_Z) \tag{3.c}$$

[19] I am grateful to Ernst Kani for the help he gave me in writing this section.

as follows from the classical *adjunction formula* of the theory of algebraic surfaces. Note that if $g_Z \geqslant 2$, then $c(\Gamma) \cdot c(\Gamma) < 0$.

There are two principles that enable us to get a handle on the collection of possible graphs Γ in $Y \times Z$.

(1) *Rigidity principle. If $g_Z \geqslant 2$, then an analytic mapping $Y \to Z$ is determined by its induced mapping on* 1-*dimensional homology*

$$H_1(Y) \to H_1(Z)$$

(*or on* 1-*dimensional cohomology*). *Equivalently*:

$$c(\Gamma) \textit{ determines } \Gamma.$$

(QUICK PROOF. Given two graphs Γ_1, Γ_2 of nonconstant functions, then as shown above, $c(\Gamma_1) \cdot c(\Gamma_1)$ is negative. But $c(\Gamma_1) \cdot c(\Gamma_1) = c(\Gamma_1) \cdot c(\Gamma_2)$ is the intersection number $\Gamma_1 \cdot \Gamma_2$, which is nonnegative, $\Gamma_1 \neq \Gamma_2$.)

(2) *Boundedness of degree. If the genus of Z is $\geqslant 2$, then any analytic nonconstant mapping from Y to Z has degree which admits an a priori upper bound* (*specifically it is bounded by the ratio*

$$\text{degree} \leqslant \frac{\chi(Y)}{\chi(Z)}$$

where χ denotes Euler characteristic).

PROOF. If $f\colon Y \to Z$ is such a nonconstant analytic mapping of degree d, then by the elementary properties of Euler characteristics,

$$\chi(Y) = d \cdot \chi(Z) - \sum_{y \in Y} (e_y - 1),$$

where e_y is the ramification index of y with respect to the mapping f. Since $\Sigma(e_y - 1) \geqslant 0$, the inequality follows.

A natural approach to obtaining the theorem of de Franchis is to use the rigidity principle, and simply to bound the number of algebraic cohomology classes $c \in H^2(Y \times Z;\, \mathbf{Z})$ which are subject to the constraints imposed by (3.a, b, c) and boundedness of the degree. Specifically, recall that an *algebraic cohomology class* in $H^2(Y \times Z;\, \mathbf{Q})$ is a $\mathbf{Q}$-linear combination of fundamental classes of curves in $Y \times Z$, and note that the desired finiteness result is an immediate consequence of:

LEMMA. *There are only a finite number of algebraic cohomology classes c in $H^2(Y \times Z;\, \mathbf{Z})$ such that*

$$(*) \qquad c \cdot \text{pt.} \times Z = a, \quad c \cdot Y \times \text{pt.} = b, \quad c \cdot c = -e$$

for given integers a, b, and e.

To see the lemma we use a bit of the theory of surfaces. If κ denotes the *canonical class* of $Y \times Z$ (which can easily be seen to be $-\chi(Z) \cdot Y \times \text{pt.} - \chi(Y) \cdot \text{pt.} \times Z$) we know that the intersection pairing on the subspace of algebraic cohomology classes perpendicular to κ is *negative-definite*. But by $(*)$ we have that

$$c \cdot \kappa = -a \cdot \chi(Y) - b \cdot \chi(Z)$$

and, in particular, $c \cdot \kappa$ is independent of c. The algebraic cohomology class $c' = (\kappa \cdot \kappa) \cdot c - (c \cdot \kappa) \cdot \kappa$ is perpendicular to κ, and $c' \cdot c'$ is a fixed (negative, immediately calculable) integer, independent of c. But by negative-definiteness, there are only a finite number of such c''s and therefore also only a finite number of c's. This concludes the proof of the lemma, and hence the theorem. But the reader might note that there is a *uniform* upper bound for the number of c's: for if L is a free abelian group of rank r with a $\mathbb{Z}$-valued negative-definite (or positive-definite) quadratic form, and if B is an integer, there is an $n(r, B)$ *depending only on r and B* which is an upper bound for the number of c's in L with $c \cdot c = B$.

There is a second approach to the theorem of de Franchis. It is more geometric and takes fewer words to describe, but it depends upon a more elaborate theory ("*Chow coordinates of curves in projective N-space*") and does not provide effective bounds.

The idea is to imbed $Y \times Z$ in $\mathbb{P}^N$ (some N) and use that the graphs Γ (as in the first approach above) have bounded degree in $\mathbb{P}^N$. Then by the theory of Chow coordinates they fall into a finite number of continuous algebraic families.

But by the rigidity principle (1) each of these continuous algebraic families reduces to a single point. Hence the set of all such Γ is finite.

b. The theorem of de Franchis-Severi. The basic idea behind this theorem [**de F, Sev**] is to associate to a given morphism f: $Y \to Z$ the composite mapping

$$\gamma_f := f^* f_*\colon H_1(Y) \overset{f_*}{\to} H_1(Z) \overset{f^*}{\to} H_1(Y)$$

and study it as a correspondence from Y to Y. Here, de Franchis and Severi prove only that there are at most a finite number of isomorphism classes of f's giving the same γ_f. This step (which was originally proved by Humbert and Castelnuovo) is, at least on the face of it, ineffective. Recently, Howard and Sommese [**H-S**], and independently Kani (whose paper will appear shortly) have produced effective versions of it.

9. On Mordell's conjecture and its analogues. Mordell made his conjecture originally for K equal to the field of rational numbers. It was a natural step to generalize it to any number field.

Lang described an analogue of Mordell's conjecture for the field of rational functions on a curve or more generally, a variety over a smaller field k. We shall give two equivalent verisons of this analogue, where we restrict ourselves to characteristic 0 even though there are analogues (somewhat harder to state) valid in all characteristics.

(**Algebraic version**) *Let k be an algebraically closed field of characteristic* 0, *and L the field of rational functions of a curve over k. Let X be a curve of genus* $\geqslant 2$ *defined over L. Then either its set of rational points* $X(L)$ *is finite, or: X is definable over k and all but a finite number of points in* $X(L)$ *are in the image of* $X(k)$.

A direct paraphrase of the above, in more geometric terms is the following.

(Geometric version) *Let k be an algebraically closed field of characteristic* 0 *and B a (not necessarily complete) smooth curve over k. Let $V \to B$ be an algebraic surface defined over k together with a surjective projection to B. For each (k-rational) point b of B, suppose that the fiber X_b is a smooth curve of genus $g \geqslant 2$. Then either $V \to B$ admits only a finite number of sections $B \to V$, or: V is a product:*

$$V = B \times X_b \quad (\textit{for any choice of point } b)$$

and all but a finite number of sections $B \to V$ are "constant sections", i.e., they project to a point in X_b.

Note that when $k = \mathbf{C}$, the last parenthetical remark boils down to the theorem of de Franchis!

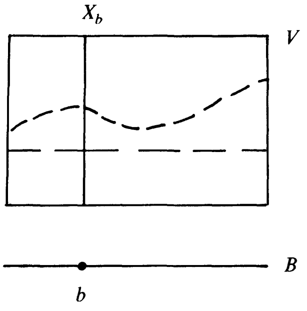


FIGURE 12

These equivalent versions were first proved (for k of characteristic 0) by Manin **[Man]**; see also **[Grau]**.[20]

III. JACOBIANS AND ABELIAN VARIETIES

1. An extension of the chord-and-tangent method to curves of genus $\geqslant 2$: the jacobian of a curve. Recall that the rule: *the sum of any three collinear points is zero* gives rise to a group law on any smooth plane cubic (positioned so that there is a unique point at infinity). A glance back at the "exercise" of II.7 will convince you, however, that a naive attempt to generalize this group structure to curves of higher degree (even quartics) will not work. For example, if on the group generated by finite formal sums of points on a plane curve of degree d you impose the equivalence relation generated by the rule: *the sum of any d collinear points is zero*, you would get too stringent an equivalence relation which would be of little use (if $d > 3$).

The useful generalization is close to this, but it has the advantage that by its very definition it is seen to be intrinsic (it depends only on the birational

[20] For higher-dimensional varieties over function fields see the recent work of Noguchi **[No]**. See also **[Des]**.

equivalence class of the curve and not upon its imbedding in the projective plane) and, moreover, three felicitous miracles occur (*analytic*, *algebraic*, and *arithmetic*) which make it an extraordinarily powerful tool.

So, let Z be any Riemann surface. By a *divisor* on the Riemann surface is meant a finite formal sum

$$(4) \qquad a_1[z_1] + a_2[z_2] + \cdots + a_m[z_m],$$

where the z_i's are points on the Riemann surface and the a_i's are integers (to be thought of as "multiplicities"). *Divisors* form a (large) abelian group, where addition is given by the obvious law. If the newcomer is struck by the bizarre use of the word *divisor* for this notion, and thinks that there must be some story behind it, he is right. (See Chapter 2 of **[Weyl]**.)

Given any nonconstant analytic mapping f: $Z \to \mathbb{P}^1$ of Z onto the Riemann sphere (or, what amounts to the same thing: any rational function) one may obtain a divisor from f (called the *divisor of zeroes-and-poles of f*) by taking

$$\sum_{z \in Z} \operatorname{ord}_z(f) \cdot [z],$$

where $\operatorname{ord}_z(f)$ is the order of vanishing of f at z if $f(z) = 0$; it is minus the order of pole of f at z if f is a pole at z; and it is zero if f has neither zero nor pole at z.

Two divisors are said to be *linearly equivalent* if their difference is the divisor of zeroes-and-poles of a nonconstant analytic mapping f. The reason for the modifier "linearly" is that any two linearly equivalent divisors fit into an algebraic family of divisors where the parameter space is $\mathbb{P}^1$, i.e., a *line*.

EXAMPLE. If X is a smooth plane curve of degree d and $Z = X(\mathbf{C})$, then any sum of d collinear points (meaning, of course, the divisor comprising the points counted with their proper multiplicities in the intersection of X with a line) is linearly equivalent to any other sum of d collinear points.

The *degree* of a divisor (4) is the sum of the multiplicities a_i. One knows that the divisor of zeroes-and-poles of any f is of degree 0.

Define the *jacobian of* Z (denoted J) to be the group of linear equivalence classes of divisors on Z of degree 0.

If z_0 is any fixed point on Z, we have a natural mapping (which we shall call the *Abel mapping based at* z_0)

$$\Phi_{z_0}\colon \quad Z \to J$$
$$z \mapsto \text{the linear equivalence class of the divisor } [z] - [z_0].$$

Clearly, J is generated as a group by the image of Z under any Abel mapping. Equally clearly, if the genus of Z is 0, then $J = 0$; otherwise any Abel mapping is injective (for if not, find an analytic mapping of degree one from Z to $\mathbb{P}^1$).

In the next three sections, we shall talk about the analytic, algebraic, and arithmetic aspects of the jacobian.

2. The analytic parametrization of J by algebraic integrals modulo periods. Recall that a Riemann surface Z of genus g possesses g, and no more than g, linearly independent everywhere holomorphic differential 1-forms. Fix such a basis of holomorphic differentials $w_1, \dots, w_g$.

Recall that the one-dimensional homology of Z is of dimension $2g$. Fix $c_1, \dots, c_{2g}$ a system of $2g$ linearly independent circuits generating the one-dimensional homology of Z.

For each circuit c_j define the *period* $\omega(c_j)$ to be the vector in $\mathbf{C}^g$ given by

$$\omega(c_j) = \left(\int_{c_j} w_1, \int_{c_j} w_2, \dots, \int_{c_j} w_g \right)$$

and define the *period lattice* Ω in $\mathbf{C}^g$ to be the subgroup generated by the periods $\omega(c_j)$ for $j = 1, \dots, 2g$.

Example. Sometimes a natural choice of systems of holomorphic differentials and circuits leaps to the eye. For instance, for the plane curve determined by the equation $y^2 = x(x-1)(x-2)(x-3)(x-4)$, the smooth model X is of genus 2, and it is tempting to take

$$\frac{dx}{y}, \quad \frac{x\,dx}{y}$$

as basis of differentials on $Z = X(\mathbf{C})$ and to choose as circuits c_j the inverse image in X of the *real* intervals:

$$0 \leqslant x \leqslant 1, \quad 1 \leqslant x \leqslant 2, \quad 2 \leqslant x \leqslant 3, \quad 3 \leqslant x \leqslant 4.$$

One can show that the period lattice Ω is *discrete* in $\mathbf{C}^g$, and a free abelian group on $2g$ generators. Therefore the quotient group $\mathbf{C}^g/\Omega$ is a (g-dimensional) complex torus.

We are now ready to describe the analytic parametrization of J by the complex torus $\mathbf{C}^g/\Omega$. Let γ be any (sufficiently smooth) directed arc in $X(\mathbf{C})$ beginning at a point x and ending at y. Define the vector in $\mathbf{C}^g$

$$\omega(\gamma) = \left(\int_{\gamma} w_1, \int_{\gamma} w_2, \dots, \int_{\gamma} w_g \right) \tag{5}$$

and note that modulo the period lattice Ω, $\omega(\gamma)$ depends only upon the points x and y and not on the directed path γ between them. A fundamental theorem is that there is an isomorphism of groups

$$J \cong \mathbf{C}^g/\Omega, \tag{6}$$

where the linear equivalence class of the divisor $[y] - [x]$ corresponds to $\omega(\gamma)$ modulo Ω. We *identify* J with the complex torus $\mathbf{C}^g/\Omega$ via this isomorphism.

The Abel mapping $\Phi_{z_0}\colon Z \to J$ is easily seen to be an analytic mapping from the Riemann surface Z to the complex torus J. Moreover, Φ_{z_0} satisfies certain *universality properties*:

(a) *Given any analytic mapping ψ from Z to A, a complex torus, such that $\psi(z_0) = 0 \in A$, there is a unique analytic homomorphism $J \xrightarrow{h} A$ such that $h \circ \Phi_{z_0} = \psi$.* (The key to this is that there are no nonconstant analytic mappings of $\mathbf{P}^1$ to a complex torus.)

(b) *The Abel mapping $Z \xrightarrow{\Phi_{z_0}} J$ induces an isomorphism on one-dimensional homology.* (It is easy to deduce this from what we have already said.)

Equivalently:

(b′) *Pullback via the Abel mapping induces a one: one correspondence between unramified finite Galois abelian coverings of the complex torus J and unramified finite Galois abelian coverings of the Riemann surface Z.*

By contemplating (4) you can convince yourself that the Abel mapping is an analytic mapping of the Riemann surface Z to the complex torus J. If $g > 0$ it is, in fact, an analytic imbedding.

Example. Since our Klein curve has such a large group of automorphisms one can show that its jacobian J (viewed as complex torus) has a particularly simple form. Specifically let $\Omega \subseteq \mathbf{C}$ denote the lattice generated by 1 and the complex number $(1 + \sqrt{-7})/2$. Then $J \cong \mathbf{C}/\Omega \times \mathbf{C}/\Omega \times \mathbf{C}/\Omega$.

It is rare that the jacobian of a curve splits up like this. But there are a few other well-known examples (for instance, the jacobian of the modular curve $X(11)$ splits—up to isogeny—into a product of twenty-six elliptic curves). For more examples see forthcoming publications of T. Ekedahl, who informs me that he has a construction of a three-parameter family of genus 9 curves whose jacobians split—up to isogeny—entirely into products of elliptic curves. For other examples see the 1985 Ph.D. thesis of Bob Kuhn [**Ku**].

Exercise. Find a different proof of the "rigidity principle" of §8 based on the analytic theory of the jacobian that we have just described.

Interlude: A theorem about Riemann surfaces equivalent to Mordell's conjecture. Let Y be a Riemann surface of genus $\geqslant 2$ and T any complex torus. Let $\varphi\colon Y \to T$ be any analytic imbedding, and let $\Gamma \subset T$ be any finitely generated group.

Some years ago Lang proved (compare [**L 4**]) that the following assertion is *equivalent* to Mordell's conjecture, and hence is now a theorem, thanks to Faltings:

Theorem. *$\varphi(Y) \cap \Gamma$ is finite.*

What is so spectacular is the extraordinary amount of algebraic geometry and arithmetic that goes into the proof of this ostensibly purely analytic assertion!

Combining the above theorem with some recent beautiful work of Raynaud (his proof of the Manin-Mumford conjecture; see also Bogomolov, Coleman) one can say even more:

If $\Gamma \subset T$ is any subgroup of the complex torus T, define the *division-point saturation* of Γ to be the group

$$\tilde{\Gamma} := [t \in T \text{ such that there is a positive integer } n \text{ with } n \cdot t \in \Gamma].$$

Note that $\tilde{\Gamma}$ contains all torsion points of T and therefore is never finitely generated.

Theorem (Faltings, Raynaud). *If Γ is finitely generated, and $\tilde{\Gamma}$ is the division-point saturation of Γ, then $\varphi(Y) \cap \tilde{\Gamma}$ is finite.*

Remark. Even when Γ is the trivial subgroup, the above theorem is deep (the Manin-Mumford conjecture: there are only a finite number of torsion points lying on any curve of genus $\geqslant 2$ analytically imbedded in a complex torus).

It would be very interesting to have some idea of what to expect in the way of uniform upper bounds. For example, is it reasonable to hope that the cardinality of the intersection $\varphi(Y) \cap \tilde{\Gamma}$ admits an upper bound that depends only on the genus of Y and the rank of Γ?

3. The algebraic nature of the jacobian. If X is a curve and J its jacobian, viewed as complex torus, then there is a holomorphic imbedding of the complex analytic manifold J in projective space of some high dimension. One may even single out a canonical *class* of such imbeddings.

For the precise definition of this canonical *class*, see Lecture III of **[Mu]**′.[21]

By Chow's theorem, any complex analytic submanifold of projective N-space is *algebraic*, i.e., is the common locus of zeroes of a finite set of homogeneous polynomial equations;

$$f_j(X_0, \dots, X_N) = 0 \qquad (j = 1, \dots, m).$$

Indeed, if V is an irreducible complex analytic submanifold of projective N-space, of codimension d, we can find a family $(f_i)_{i=1,\dots,m}$ of homogeneous polynomial equations whose common locus of zeroes is V and such that for every point $v \in V$ there are d equations $g_1, \dots, g_d$ in that family such that the $N \times d$ matrix $\partial g_i/\partial X_k|_v$ has rank d. Such a family $(f_i)_{i=1,\dots,m}$ we shall call a *defining set of equations* for V.

Any complex torus which is *algebraic* in the above sense, i.e., which is the locus of zeroes of a defining set of equations, is called an *abelian variety*.

In particular, the jacobian J of an algebraic curve X is an abelian variety: it has defining sets of equations for the projective imbeddings (in its canonical class).

The reader should be warned, though, that these defining sets of equations are difficult to produce and it would be bad news if we were ever obliged to explicitly "inspect" such a defining set of equations when the genus is > 1. The most noteworthy achievement in this direction is Mumford's beautiful paper **[M 2]** in which, for certain classes of projective imbeddings he explicitly produces such a defining set for any abelian variety, where each of the defining equations is of degree two; in particular, any abelian variety can be realized as an intersection of quadrics in a suitable dimensional projective space. The classical fact that any elliptic curve may be represented as the intersection of two quadrics in $\mathbb{P}^3$ is a special case of this.

Digression on polarizations. The question of imbeddings of complex tori in projective space is related to *polarization*, a notion which bears upon many of the results we shall be discussing later. To give some idea of one of the most important uses of polarizations, we shall define a *polarization class of projective imbeddings*[22] of a complex torus T. *A polarization class* $\{T \to \mathbb{P}^N\}$ is a family of holomorphic imbeddings in projective N-space, any member of which can be obtained from any other by composition on the left by a suitable translation

[21] An imbedding $J \subseteq \mathbb{P}^N$ is in the canonical class alluded to above if, as $H \subset \mathbb{P}^N$ runs through all hyperplanes, $H \cap J$ runs through all effective divisors in J which are linearly equivalent to (some fixed translate of) *three times* the Riemann θ-divisor. See **[Mu]**′ for details.

[22] A neologism.

of T, and on the right by a suitable projective linear automorphism of $\mathbb{P}^N$, and moreover, if $T \to \mathbb{P}^N$ is a given member of the family, we require that as $H \subseteq \mathbb{P}^N$ runs through all hyperplanes, $H \cap T$ runs through *all* effective divisors which are linearly equivalent to a fixed divisor in T. Given, then, a polarization class of projective imbeddings of T, one has a family of effective divisors (the intersections with hyperplanes) any one of which is, after suitable translation in T, linearly equivalent to any other. This family of effective divisors uniquely determines the polarization class of projective imbeddings from which it arose as intersections with hyperplanes.

One can define a *polarization* as an equivalence class of divisors $\{D\}$ in T under the equivalence relation generated by translation and linear equivalence, such that for some positive integer M the equivalence class $\{M \cdot D\}$ containing divisors which are M times D comes from a polarization class of projective imbeddings (by intersection with hyperplanes) as above.[23]

What makes the notion of polarization manageable is the theorem (cf. §I of **[M 3]**) which asserts that if $T = V/L$ is a complex torus obtained as the quotient of the complex vector space V by the lattice L, polarizations of T as above are in natural one:one correspondence with positive definite Hermitian forms

$$H: V \times V \to \mathbb{C}$$

which have the property that if $E = \operatorname{im}(H)$ is the imaginary part of H, then E restricted to $L \times L$ takes values in $\mathbb{Z} \subset \mathbb{C}$. For later reference, define the *degree* of the polarization determined by H to be the *determinant* of the bilinear pairing E: $L \times L \to \mathbb{Z}$ (compare the discussion at the end of Chapter III in **[M 3]**).

The polarization of a jacobian given by the equivalence class of the Riemann θ-divisor (cf. **[M 3]**) is of degree 1.

EXAMPLE (*The polarization on the jacobian of the Klein curve*). We have already described in §2 above, the lattice Ω^3 in $\mathbb{C}^3$ determining the jacobian of the Klein curve. Here we shall give a slightly different, but equivalent, lattice with respect to which the polarization is easily described, along with its full group of 336 automorphisms.

Let $\alpha = (1 + \sqrt{-7})/2$ and let $\bar{\alpha}$ denote the complex conjugate of α so that $\alpha\bar{\alpha} = 2$. Let $R = \mathbb{Z}[\alpha]$ be viewed as a subring of the complex numbers, so that, indeed, R is the lattice Ω of the example of §2. Let Λ denote the lattice in $\mathbb{C}^3$ defined as the sublattice of $R^3 \subset \mathbb{C}^3$, of index eight, comprising all vectors $x = (x_1, x_2, x_3) \in R^3$ such that

$$x_1 \equiv x_2 \equiv x_3 \equiv 0 \bmod \alpha \quad \text{and} \quad x_1 + x_2 + x_3 \equiv 0 \bmod \bar{\alpha}.$$

One checks that if $\bar{x} \cdot y$ denotes the standard Hermitian inner product on $\mathbb{C}^3$, then if $x, y \in \Lambda$, we have $\bar{x} \cdot y \in 2 \cdot R$.

Define:

$$(x, y) := \bar{x} \cdot y/2.$$

[23] E.g., if J is the jacobian of a curve X, a Riemann θ-divisor (cf. **[Mu]**′) yields a *polarization* of J; the "canonical polarization class of projective imbeddings" discussed in the previous footnote is determined by 3 times the Riemann θ-divisor.

Then (x, y) restricts to a Hermitian form on Λ with values in R and of discriminant 1 (because it is of discriminant $1/8$ on R^3).

It is this Hermitian form (normalized by division by $\sqrt{7}/2$, which is the area of a fundamental domain for Ω) which gives rise to the polarization coming from the Riemann divisor on the jacobian of the Klein curve. Note that there are 42 vectors e in Λ such that $(e, e) = 2$; these come from coordinate permutations and sign changes applied to the vectors $(2, 0, 0)$, $(\alpha, \alpha, 0)$, and $(\bar{\alpha}, 1, 1)$. The group generated by the (21 distinct) reflections $y \mapsto y - (e, y)e$ coming from these 42 vectors is the full group (isomorphic to $(\pm 1) \times \mathbf{PSL}_2(\mathbb{F}_7)$) of automorphisms of Λ preserving the Hermitian form (,). I am grateful to Serre for providing me with this example.

A theorem of Torelli asserts that the isomorphism class of a smooth projective curve over $\mathbf{C}$ is determined by the isomorphism class of its jacobian, taken together with its polarization.

Weil's proof of Torelli's theorem gives the following sharper statement:[24]

(1) ("*hyperelliptic case*") *Let C_1 and C_2 be smooth complete curves of genus $\geqslant 2$ over $\mathbf{C}$ which are hyperelliptic, i.e., they can be expressed as double covers of the projective line. Then the set of isomorphisms from C_1 to C_2 is in natural one*: *one correspondence with the set of isomorphisms from the polarized jacobian of C_1 to the polarized jacobian of C_2.*

(2) ("*nonhyperelliptic case*") *Let C_1 and C_2 be smooth complete curves over $\mathbf{C}$ which are nonhyperelliptic. Let f be an isomorphism of the polarized jacobian of C_1 onto the polarized jacobian of C_2. Then either $+f$ or $-f$ is induced from an isomorphism of C_1 onto C_2 (and not both). This establishes a one*: *one correspondence between the isomorphisms of C_1 onto C_2 and half of the isomorphisms from the polarized jacobian of C_1 onto the polarized jacobian of C_2.*

EXAMPLE. The Klein curve over $\mathbf{C}$ is not hyperelliptic. Its group of automorphisms is $\mathbf{PSL}_2(\mathbb{F}_7)$ while the group of automorphisms of its polarized jacobian is $(\pm 1) \times \mathbf{PSL}_2(\mathbb{F}_7)$.

The use of Torelli's theorem plays a key role in the work of Zarhin-Parshin and of Faltings for it allows them to *replace* curves by their polarized abelian varieties, with no loss of information, and thereby to translate Diophantine questions about curves to questions about abelian varieties.

The Torelli theorem brings to mind a natural question: Does the complex torus J itself (stripped, so to speak, of its canonical class of projective imbeddings) determine the isomorphism class of the algebraic curve X? The answer is: *Almost*! There are only a finite number of isomorphism classes of curves whose jacobians are isomorphic to any given complex torus (compare [**De**, 1.25, 1.26]′ and [**Na-No**]). For examples of different (genus two) curves with the same jacobian (stripped of polarization), see [**Ha-Ni**] and [**Hay**].

4. The arithmetic nature of the jacobian. Suppose you are given any complex analytic submanifold M in $\mathbb{P}^N(\mathbf{C})$. Then by "Chow's theorem" M admits a defining set of equations $(f_j = 0)_j$. Say that M is *defined over K* (a subfield of $\mathbf{C}$) if you can find such a defining set of equations all of whose coefficients lie

[24] There is an analogous statement valid over any field.

in K. There is no difficulty in guessing what should be meant by an analytic mapping (between two complex analytic submanifolds in $\mathbb{P}^N(\mathbb{C})$ and $\mathbb{P}^{N'}(\mathbb{C})$, respectively) to be *defined over* K—as in the case of Riemann surfaces (II.§4), one asks that the graph of the mapping admit a defining set of equations with coefficients in K. One can therefore also talk of *isomorphism over* K.

If A is a complex torus in $\mathbb{P}^N(\mathbb{C})$, that is, an abelian variety, we say that *the abelian variety A is defined over K* if as a complex analytic submanifold it is defined over K *and* if its origin is a K-rational point in projective space.

Essentially by virtue of the fact that the group law on a complex torus is *determined by* the complex analytic structure alone, together with a choice of base-point (to be taken as origin), it turns out that if an abelian variety A is defined over K, then its group addition law $A \times A \to A$ and its inverse law are both also defined over K. Consequently, its set of K-rational points, $A(K)$, is a subgroup of $A(\mathbb{C})$. The Mordell-Weil theorem, already encountered for algebraic curves of genus 1, holds in the more general context of abelian varieties defined over number fields:

THEOREM. *If A is an abelian variety defined over K, where K is the field of rational numbers, or more generally, a number field, then the group of K-rational points $A(K)$ is finitely generated. That is*:

$$A(K) \cong \mathbb{Z}^r \oplus [\textit{finite abelian group}].$$

Now suppose given an algebraic curve X defined over a subfield K in $\mathbb{C}$. The jacobian J may then be shown to possess a projective imbedding (in its "canonical" class) which gives it the structure of (polarized) abelian variety defined over (the same field) K.

Although on the face of it, what has just been said may seem natural enough, it is worth pausing to absorb its implications for the simplest case of curves of genus 1. Let, then, X be an algebraic curve of genus 1 defined over K and J its jacobian. If X possesses a K-rational point x_0, then an Abel mapping Φ_{x_0}: $X(\mathbb{C}) \to J$ is defined over K and yields a K-isomorphism between X and J. But if X does not possess any such K-rational point, then J is surely *not* K-isomorphic to X (since J always has, at least, the origin as K-rational point); i.e., J is *another* curve.

Integral structure. Now let us restrict attention to K a number field. Very little will, in fact, be lost if you think of K as the field of rational numbers. Let $\mathcal{O} \subset K$ be the ring of algebraic integers in K (e.g., if $K = \mathbb{Q}$, then $\mathcal{O}$ is just the ring of ordinary integers). Let $P \subset \mathcal{O}$ be a maximal ideal (e.g., if $\mathcal{O} = \mathbb{Z}$, then P is generated by p a prime number).

Let $k = \mathcal{O}/P$, the quotient field (e.g., the integers modulo p).

A complex submanifold $M \subset \mathbb{P}^N(\mathbb{C})$ defined over K is said to have *good reduction at P as imbedded in* $\mathbb{P}^N(\mathbb{C})$ if it has a defining set of equations $(f_j = 0)_j$ all of whose coefficients lie in $\mathcal{O}$ and such that if we pass to the quotient field $k = \mathcal{O}/P$ by taking $\bar{f}_j$ to be f_j with coefficients considered only modulo P, then the set of equations $(\bar{f}_j = 0)_j$ define a smooth algebraic variety over k of the same dimension as M. This boils down to requiring that the matrix $(\partial \bar{f}_j/\partial u_k)_{j,k}$ have rank equal to the dimension of M at all points in the locus of common zeroes of $(\bar{f}_j)_j$ in $\mathbf{P}^N(\bar{k})$ where $\bar{k}$ is an algebraic closure of k.

For example: The Klein curve is defined by the homogeneous form $f = X^3Y + Y^3Z + Z^3X$ which has coefficients in $\mathbf{Z}$ and which reduces modulo p to a smooth plane curve over the field of integers mod p, for all primes $p \neq 7$ (easy computation). So the Klein curve has good reduction as imbedded in the projective plane, at all primes $p \neq 7$.[25]

As we introduced it, the notion of having good reduction at P is with reference to a specific imbedding in $\mathbf{P}^N(\mathbf{C})$. We can cut loose from any fixed imbedding by saying that an algebraic curve X defined over K (or an abelian variety A defined over K) has *good reduction at P* if X is K-isomorphic to an algebraic curve in some $\mathbf{P}^N(\mathbf{C})$ with good reduction at P (or A is isomorphic to an abelian variety in $\mathbf{P}^N(\mathbf{C})$ with good reduction at P) in the sense described above.

Having good reduction is the "general rule" in the sense that if $M \subset \mathbf{P}^N(\mathbf{C})$ is a complex analytic submanifold defined over K, then M has good reduction even as imbedded in $\mathbf{P}^N(\mathbf{C})$ at all but a finite number of prime ideals P.

The link between good reduction of curves and good reduction of their jacobians, considered as polarized abelian varieties is reasonably good: If X is defined over K and has good reduction at P, then its jacobian is defined over K and has good reduction at P as imbedded in $\mathbf{P}^N(\mathbf{C})$ via any projective imbedding in its "canonical" class.

The converse, however, is not necessarily true, i.e., there is a smooth curve over K whose jacobian has good reduction at P and yet the curve X itself does not have good reduction at P.

For example, let p be a prime number $\geqslant 5$; let $\mathcal{O}$ be the ring of integers in $K = \mathbf{Q}(\sqrt{p})$; and let P be the prime ideal generated by $\sqrt{p}$.

Take X to be the curve of genus 2 over K given by the model over $\mathcal{O}$:

$$y^2 = (x + 2)(x + 1)x(x + \alpha p)(x + \beta p),$$

where α, β, 0, 1, 2 are all integers, distinct mod p.

The reduction mod p of the above model is a curve with a cuspidal singularity at $(x, y) = (0, 0)$. The smooth model of this curve is the curve, E_1, of genus 1 given by the equation $y^2 = (x + 2)(x + 1)x \bmod p$.

But a "blow-up" of our model over $\mathcal{O}$ (at the point $(x, y) = (0, 0)$ in characteristic p) gives us another model whose characteristic p fiber is a *union* of two curves of genus 1, E_1, and a "new one", E_2, given by the equation $y^2 = x(x + \alpha)(x + \beta)$.

[25] With a suitable imbedding of the Klein curve in projective space, and working over a number field sufficiently ramified at 7 one can produce a model for it which has good reduction also at the primes dividing 7. Indeed, Serre informed me that the reduction "modulo 7" of the Klein curve is the projective model of the hyperelliptic curve $y^2 = u^7 - u$. The action of the simple group $\mathbf{PSL}_2(\mathbf{F}_7)$ on this curve is the evident action obtained by viewing the curve as the double cover of the projective line over $\mathbf{F}_7$ whose ramification points are precisely the eight points in $\mathbf{P}^1(\mathbf{F}_7)$.

The jacobian of X over k has good reduction at p, where the fiber of its smooth model in characteristic p is isomorphic to the *product* of E_1 and E_2.

IV. CLASSIFICATION OF FAMILIES WITH BOUNDED BAD REDUCTION

1. Kodaira's problem. Consider a family of Riemann surfaces of genus g parametrized by the complement of a finite set S in the projective line (Figure 13).

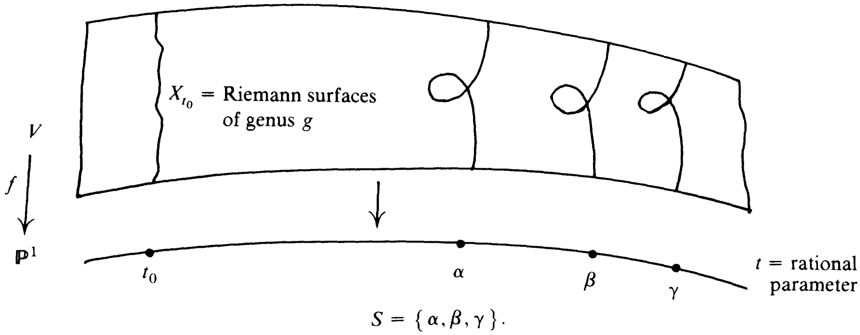

X_{t_0} = Riemann surfaces of genus g
V
f
$\mathbb{P}^1$
t_0
α
β
γ
t = rational parameter
$S = \{\alpha, \beta, \gamma\}$.

FIGURE 13

We assume that the family varies "analytically" in the sense that the various fibers sweep out an irreducible analytic variety V and the mapping f is analytic. We also assume that the family is *truly varying* in the sense that not all the fibers are isomorphic (as Riemann surfaces). We shall refer to the finite set S as a *bound for the bad reduction* of the family. Kodaira's problem is to classify all families of fiber genus g with bad reduction bounded by a given set S.

EXAMPLE. Consider the family of curves of genus one:

$$Y^2 = X^3 + X + t.$$

The negative of the discriminant of the above equation is $4 + 27t^2$ and consequently the bad reduction of the family is bounded by the set S consisting of the three points $(\infty, \pm 2/3\sqrt{3})$. It is a general fact that any truly varying family must have at least three points of bad reduction over $\mathbb{P}^1$ (cf. Beauville's exposé #6 in **[Szp 3]** for a quick proof of this well-known result, and for a discussion of related matters, among which being the situation in characteristic $p > 0$ where the analogous result is no longer true).

In contrast to what happens over the base $\mathbb{P}^1$, Kodaira produced "truly varying" families $V \to B$ of Riemann surfaces of genus g (> 1) over a compact base Riemann surface (of genus > 1) with no bad reduction (i.e., where the set S may be taken to be empty). He did this, roughly, as follows:

Step 1. If F is any Riemann surface of genus > 0, and $P \in F$ is a point on it, there is a finite connected covering $F' \to F$ unramified outside P and ramified at P. For example, we shall restrict our attention to the subclass of such coverings of degree four which are obtained by first taking a connected unramified covering $F'' \to F$ of degree 2 and then taking a connected covering $F' \to F''$ of degree 2 unramified outside the inverse image of P, but definitely ramified. There are only a finite number of coverings in this subclass.

Step 2. Let B be a compact Riemann surface (the candidate for our base) and let $f\colon B \to F$ be a nonconstant mapping. For each $b \in B$, denote by $P_b \in F$ the image of b under f. There are a finite number of coverings $F_b' \to F$ of degree four, as specified in Step 1 above, unramified outside P_b and ramified at P_b.

Step 3. We seek to make a coherent global choice of those coverings $F_b' \to F$ for b varying in B. This may not be possible globally over B, but after a finite base change $B' \to B$, it can be done. This gives us an analytic family $V = (F_{b'}')_{b' \in B'}$ of curves parametrized by B'. The fibers $F_{b'}'$ are all nonsingular. Suppose that F is of genus > 1. The family is "truly varying" as can be seen by the fact that the locus of ramification of $F_{b'}' \to F$ is "truly varying".

Kodaira's construction may be viewed as the precursor of Parshin's construction, to be given in §3 below.

2. Shafarevich's problems. It was Shafarevich in his 1962 address at the International Congress of Mathematicians in Stockholm who first called attention to the following important analogue of Kodaira's Problem, and who perceived its Diophantine importance:

Shafarevich's problem for curves. *Let S be a finite set of prime ideals in $\mathcal{O}$ the ring of integers of the number field K. Let $g \geqslant 0$.*

How many distinct K-isomorphism classes of curves X/K are there, of genus $g \geqslant 2$ and possessing good reduction at all primes $P \notin S$?

Shafarevich's problem for abelian varieties. *How many K-isomorphism classes of abelian varieties of dimension g are there, defined over K, with good reduction at all primes $P \notin S$?*

"**Shafarevich's conjecture**" is the assertion that in both cases, there are only a finite number.[26]

By a refinement of Torelli's theorem and the discussion in §3 one shows that if Shafarevich's conjecture is true for abelian varieties, then it is true for curves of genus $\geqslant 2$. The work of Faltings **[Fa]** (with a slight improvement given by Zarhin [**Zar 4**]) established the conjecture:

THEOREM (SHAFAREVICH'S CONJECTURE). *Let K be a number field, and S a finite set of prime ideals in the ring of integers of K.*

There are only a finite number of K-isomorphism classes of algebraic curves X of genus $g \geqslant 2$ defined over K and possessing good reduction outside S.

REMARKS. 1. *Prior work in the function field case.* Replacing K by a field of rational functions on a curve B over $\mathbb{C}$. Shafarevich's problem for curves

[26] Although these assertions are generally referred to as Shafarevich's conjecture, Shafarevich only made the conjecture for curves in print. The first appearances of the conjecture for abelian varieties occurred in the a priori weaker form where the abelian varieties were required to be polarizable with a polarization of bounded degree (cf. [**Se 4**] for abelian surfaces and [**Par 2**]). The equivalence between the weaker and the full form of the conjecture for abelian varieties is obtained by something called "Zarhin's trick" (cf. [**Zar 4**]). See also [**De**]′ for a discussion of polarizations.

(which then coincides with Kodaira's problem) was resolved by Arakelov in 1971 [**Ara**]. Specifically, he showed that for a fixed genus $g \geqslant 2$ and finite set S of points in B there are only a finite number of truly varying families of curves of genus g over B with bad reduction bounded by S. Arakelov's method is to prove a rigidity result (resembling the "second approach" to the theorem of de Franchis discussed in II.8.a above) for maps of $B - S$ into the moduli space of curves of genus g. See the account of this in lecture II of [**Mu**]$'$.

2. *The case of curves of genus one.* A curve of genus one over K may or may not possess a K-rational point. If the curve does have a K-rational point, and if we fix such a point as "origin", there is a unique way of endowing the curves with the structure of a K-rational group law with identity element as the chosen origin. Thus a curve of genus one over K with a fixed K-rational point gives rise to an abelian variety of dimension one over K, i.e., an elliptic curve.

Shafarevich was the first to prove that there are only a finite number of K-isomorphism classes of elliptic curves over K with good reduction outside S [**Shaf**].

It is interesting to note that the question of classification of *curves of genus one over K with good reduction outside S* has a somewhat different status from the finiteness questions answered by the above theorem. Firstly, there are examples of number fields K and finite (nonempty) sets S such that an infinite number of genus one curves over K possessing good reduction outside S can be found, mutually nonisomorphic (over K).

More precisely, if $K = \mathbf{Q}$ and S is any finite set of primes for which there exists an elliptic curve over $\mathbf{Q}$ possessing only a finite number of $\mathbf{Q}$-rational points, and having good reduction outside S, then there are an infinity of mutually nonisomorphic curves of genus one over $\mathbf{Q}$ possessing good reduction outside S.[27]

There are such examples if S contains 2 or if it contains 3, or 7, or 11, or 17, or 19, or 37, ...

Secondly, if S is empty, we await a different answer: the well-known conjecture of Shafarevich-Tate (for elliptic curves) together with the theorem of Shafarevich whose proof we shall give below imply:

CONJECTURE. *There are only a finite number of K-isomorphism classes of genus one curves over K with everywhere good reduction.*

Here is Shafarevich's argument which proves the finiteness of the number of K-isomorphism classes of elliptic curves defined over K and possessing good reduction outside a finite set of primes S of K. For minor reasons, we give it only in the case $K = \mathbf{Q}$. Any $\mathbf{Q}$-isomorphism class of elliptic curves with bad

[27] If E is an elliptic curve over $\mathbf{Q}$ with good reduction outside S and Mordell-Weil group finite, Tate provided the following argument to show that the group of principal homogeneous spaces for E over $\mathbf{Q}$, trivial at nonarchimedean primes outside S, is infinite.

First, S is nonempty, by Tate's theorem (see "*examples*" below). Next, if p is a prime in S, we may suppose that the p-primary part of the Shafarevich-Tate group is finite; otherwise we are done.

Now use finiteness of both the Mordell-Weil group and the p-part of the Shafarevich-Tate group to evaluate the relevant portion of the exact sequence on p. 293 of [**Ta**].

reduction bounded by S can be given a model of the form:

$$y^2 = x^3 + ax + b$$

with a, b in $\mathbb{Z}$ and such that the discriminant,

$$\Delta = -27b^2 - 4a^3,$$

is divisible only by prime numbers in the set $S \cup \{2,3\}$. Since a suitable change of coordinates enables one to produce a model whose discriminant Δ is not divisible by any perfect sixth power, the coefficients a, b of our models are constrained to be integral solutions of a finite number of "generalized cubic discriminant equations" (see the Digression at the end of Part I):

$$-4A^3 - 27B^2 = M,$$

where M ranges through all integers divisible only by primes in $S \cup \{2,3\}$ and free of perfect sixth powers. But (by Siegel's theorem, or, effectively, by Baker-Stark; see the Digression) each of these generalized cubic discriminant equations *has only a finite number of integral solutions*, and consequently there are only a finite number of isomorphism classes of elliptic curves over $\mathbf{Q}$ with bad reduction bounded by S.

Since Siegel's theorem played a central role in Shafarevich's proof in the case of genus 1, the sentiment had, at times, been expressed (before Faltings' work) that a fruitful path to the general Shafarevich conjecture might be by establishing a vastly more general higher-dimensional analogue of Siegel's theorem. This line of attack, formidable though it seems, may ultimately be viable (see the discussion in [**Par 1**]). Nevertheless, Faltings' work has offered the option of totally reversing directions! That is, instead of using Siegel's theorem to establish the genus 1 case of the above Shafarevich conjecture, one may choose to first establish this conjecture via Faltings' methods and then *apply it* to deduce Siegel's theorem! This has indeed been done [**F-W**, Chapter V, §5].

EXAMPLES. **Explicit classification.** The fact that there are only a finite number of K-isomorphism classes of algebraic curves of genus g, defined over K, and with bad reduction bounded by S raises the prospect of giving complete lists in some important cases. For example, by refining the methods used by Shafarevich in the case of elliptic curves, Tate was able to show that there are no elliptic curves defined over $\mathbf{Q}$ and possessing everywhere good reduction. Just this past year, Fontaine has proved the much more general result that there are *no* nontrivial abelian varieties and *only one curve* ($\mathbf{P}^1$) defined over $\mathbf{Q}$ and possessing everywhere good reduction [**Fon**].[28] This result had been conjectured by Shafarevich [**Shaf**].

Some years ago Grothendieck commented that the only algebraic varieties (of any sort) that come to mind which are defined over $\mathbf{Q}$ and possess good reduction at all primes are birationally equivalent to homogeneous spaces of

[28] Serre has pointed out that standard conjectures concerning the relevant L-functions and their functional equations have strong implications concerning the minimal conductor that an abelian variety of dimension $d > 0$ over $\mathbf{Q}$ can have. Mestre has refined this argument to show (modulo these standard conjectures) that this minimal conductor is $> 10^d$, which is a remarkably sharp bound in that we have examples (e.g., $X_0(11)^d$) with conductor 11^d.

linear algebraic groups. Nevertheless, even at present, it would be difficult to frame any general conjectures along these lines with firm conviction.[29]

Returning to the case of elliptic curves defined over $\mathbf{Q}$, but with bad reduction bounded by a given set S, the Weil-Tanyama conjecture asserts that any such elliptic curve is the quotient of the modular curve $X_0(N)$, where N can be explicitly given in terms of S. This enables us to (conjecturally) produce a complete list for many S. For the interesting case of $S = \{11\}$, see **[A-C-H-P]** and **[Se 2]**.

3. Parshin's construction: Shafarevich's conjecture implies Mordell's conjecture. The easiest way to understand the role played by Parshin's beautiful idea is to first consider the idea, divested of any detail.

To any triple (g, K, S) where g is a "genus" $\geqslant 2$, K is a number field, and S a finite set of primes in K, Parshin associates another such triple (g', K', S') and he defines a mapping:

$$(*)\qquad \left\{\begin{array}{l} K\text{-isomorphism classes of}\\ \text{pairs } (X, P) \text{ where } X \text{ is a}\\ \text{curve of genus } g \text{ defined}\\ \text{over } K \text{ and having good}\\ \text{reduction outside } S\text{, and } P\\ \text{is a } K\text{-rational point on } X \end{array}\right\} \xrightarrow{\alpha} \left\{\begin{array}{l} K'\text{-isomorphism classes}\\ \text{of curves } X' \text{ of genus } g'\\ \text{defined over } K' \text{ and}\\ \text{having good reduction}\\ \text{outside } S' \end{array}\right\}.$$

Parshin shows that his mapping is finite-to-one.

Having done this, it is evident that Shafarevich's conjecture implies Mordell's conjecture. For, fix any curve X of genus $g \geqslant 2$ defined over K. There is a finite S of primes of K bounding the bad reduction of X. Now, let P range through all K-rational points of X. For each such P, Parshin's construction α yields a K'-isomorphism class $X' = X_P$ of genus g' curve defined over K' with bad reduction bounded by S'.

But Shafarevich's conjecture affirms that there are only a finite number of such X''s. Since α is finite-to-one, there are then only a finite number of such P's.

It remains to sketch the definition of the mapping α, and to explain why it is finite-to-one. Before we begin, it should be remarked that the construction per se is somewhat ad hoc. There are a number of slightly different constructions, each with advantages and disadvantages. Here is one construction, given in two steps below.

Step 1. Let Z be any compact Riemann surface of genus > 1 and $Z^{(2)} \to Z$ the maximal connected (unramified) covering space which is Galois, with Galois group G abelian of exponent 2 (i.e., the square of every element in G is trivial).

[29] Especially so since newforms of level 1 (e.g., the classical modular form Δ of weight 12) yield nontrivial *motives* having everywhere good reduction.

One way of realizing such a covering is to use the universality property (b′) of the jacobian:

Choose a point $z_0 \in Z$ and consider the pullback

$$\begin{tikzcd} Z^{(2)} \arrow[r] \arrow[d] & Z \arrow[d, "\Phi_{z_0}"] \\ J \arrow[r, "\text{``2''}"] & J \end{tikzcd}$$

where "2" means "multiplication by 2" in J, the jacobian of Z.

Since the first Betti number of Z is $2g$, $Z^{(2)}$ is a Galois covering of Z of order 2^{2g}. The genus of $Z^{(2)}$ is $(g-1)\cdot 2^{2g}+1$.

Now suppose that $Z = X(\mathbf{C})$ is the Riemann surface associated to an algebraic curve X defined over K possessing good reduction outside S. Let S_2 denote the union of S with the set of all primes of K "lying over 2" (i.e., prime ideals containing the integer 2). One can show that there is an algebraic curve $X^{(2)}$ defined over K, possessing good reduction outside S_2 whose Riemann surface is $Z^{(2)}$, and the covering $X^{(2)} \to X$ is defined over K.

So far the rational point P has not entered into the construction.

Step 2. Let us now fix (K, S, g) and give ourselves a pair (X, P) as in the display $(*)$. Let $Z = X(\mathbf{C})$. Let $D_P \subset Z^{(2)}$ denote the full inverse image of the point P. There are, therefore, 2^{2g} points in D_p. We seek a Riemann surface covering

$$Z_P \to Z^{(2)}$$

which is of degree two, and which is ramified at the points of D_P and nowhere else. By Riemann surface theory one shows that such a covering exists. Its genus can be computed to be $g' = (g-1)2^{2g+1} + 2^{2g-1} + 1$.

Moreover, by some standard algebraic geometric arguments and elementary algebraic number theory, one shows that there is a field K' which depends only on the triple (K, S, g) such that Z_P is the Riemann surface of an algebraic curve X_P defined over K', possessing good reduction outside S' = the set of primes of K lying over S_2. Choosing such an X_P for each (X, P) gives the ad hoc mapping

$$(X, P) \overset{\alpha}{\to} X_P.$$

Now let $g \geqslant 2$. Why is the ad hoc mapping finite-to-one for any fixed X? The answer is given by the geometry of X_P and X. The mapping $X_P \to X$ is ramified over precisely one point of X; namely P. If there were an infinity of points P such that X_P were isomorphic (say, to the same curve Y) then there would be an infinity of *different* mappings of Y onto X, *violating de Franchis' theorem*.

V. HEIGHTS

1. Height of points. Points of the projective plane may be viewed as lines through the origin in 3-space, and a rational point α, i.e., a point of $\mathbf{P}^2(\mathbf{Q})$ may be viewed as a line which contains at least one (and hence an infinity) of nonzero *integral* lattice points, i.e., points (a, b, c) where a, b, and c are integers. Define the *height* of such a point to be the logarithm of the distance to zero of the closest nonzero integral lattice point on α. Equivalently,

$$h(\alpha) = \log\sqrt{a^2 + b^2 + c^2},$$

where (a, b, c) is a nonzero integral point on α such that a, b, and c have no common factors.

(picture in $\mathbb{P}^1(\mathbb{Q})$)

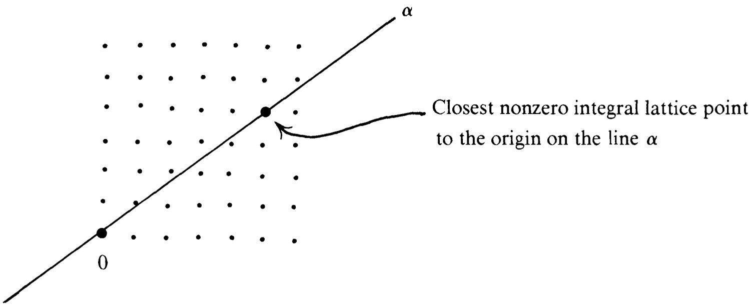

α
Closest nonzero integral lattice point to the origin on the line α
0

FIGURE 14

Since there are only a finite number of integral lattice points in any ball of finite radius,

> *Given any real number B, there are only a finite number of points $\alpha \in \mathbb{P}^2(\mathbb{Q})$ of height $\leqslant B$.*

If T: $\mathbb{P}^2 \to \mathbb{P}^2$ is any projective linear transformation, then T does not preserve height, but it almost does:

> $|h(T(\alpha)) - h(\alpha)|$ *is a bounded function of* $\alpha \in \mathbb{P}^2(\mathbb{Q})$ [elementary exercise].

Now if $C \subset \mathbb{P}^2$ is a plane curve, the restriction of the height function to $C(\mathbb{Q})$, defines *the height of a rational point on C* and hence also on X.

Visible example. Turn back to our list of rational points on the plane curve $y^2 + y = x^3 - x$ (Subexample 1 of II.7). As Tate once remarked, a rough measure for the height of such a point is the length of line on the page that it takes to write the point (expressed as a fraction in lowest terms, of course).

Now let C be a plane curve of degree d defined over $\mathbb{Q}$ with X as smooth model. Let $C(\mathbb{Q})_B$ be the subset of rational points of height $\leqslant \log B$. Then $C(\mathbb{Q})_B$ is finite; denote its cardinality by $|C(\mathbb{Q})_B|$. We have the following asymptotic behavior for $|C(\mathbb{Q})_B|$:

Either $X(\mathbb{Q})$ is empty or:
Genus 0: $|C(\mathbb{Q})_B| = c \cdot B^{2/d} + O(B^{1/d}\log B)$ with $c > 0$.
Genus 1: $|C(\mathbb{Q})_B| = c \cdot (\log B)^{r/2} + O((\log B)^{(r-1)/2})$.
Genus 2: $|C(\mathbb{Q})_B| = O(1)$ (by Faltings).[30]

[30] Before Faltings, one had the bound $|C(\mathbb{Q})_B| = O(\log\log B)$ by a theorem of Mumford to be discussed presently.

In the genus 1 case the constant r is the rank of the Mordell-Weil group of the jacobian J of the smooth model X, i.e., r is that number such that $J(\mathbf{Q})$ is isomorphic to $\mathbb{Z}^r \oplus$ [finite group]. The constant c appearing in the asymptotic genus 1 formula is also an important arithmetic invariant of the situation. It is a positive number, very likely a transcendental number if $r > 0$. It is easily expressible in terms of the degree d, and the *regulator* of J, a quantity to be introduced later.

Of course there is a natural generalization of the notion of height to projective space of any dimension, and consequently, by restriction we obtain a *height function* on polarized abelian varieties over $\mathbf{Q}$. We shall again denote this function by h:

$$J(\mathbf{Q}) \underset{h}{\rightarrow} \mathbb{R}.$$

A natural question to ask is: How does the height function behave with respect to the group structure on $J(\mathbf{Q})$?

Answer (*Néron-Tate*). It is essentially quadratic! That is,[31] there is a unique bilinear, symmetric (positive-definite) pairing

$$\begin{gathered} J(\mathbf{Q}) \times J(\mathbf{Q}) \rightarrow \mathbb{R} \\ (u,v) \rightarrow \langle u,v \rangle \end{gathered}$$

(*the Néron-Tate canonical height pairing*)

such that $|h(\alpha) - \langle \alpha,\alpha \rangle|$ is a bounded function on $J(\mathbf{Q})$.

If we denote by $\hat{h}$ the quadratic function $\hat{h}(\alpha) = \langle \alpha,\alpha \rangle$, then $\hat{h}$ can be directly computed from h by the formula

$$\hat{h}(\alpha) = \lim_{N \rightarrow \infty} h(2^N \cdot \alpha)/2^{2N}$$

and, of course, the bilinear form $\langle \alpha,\beta \rangle$ can be reconstructed in the usual way from its associated quadratic function $\hat{h}$.

The visible example again. Tate has pointed out that the essential quadraticity of the height is sometimes clearly visible in the profile of the data. Go back to our list of rational points for $y^2 + y = x^3 - x$ (subexample of II.7) and note the shadow of a parabola on the page!

Since the Néron-Tate canonical height pairing is also positive-definite, if $P_1, \ldots, P_r$ is a basis for $J(\mathbf{Q})$ modulo torsion, there is a natural *Euclidean space structure* on the r-dimensional real vector space $P_1 \cdot \mathbb{R} \oplus P_2 \cdot \mathbb{R} \oplus \cdots \oplus P_r \cdot \mathbb{R}$ with inner product given by the canonical height pairing. Or, to turn it around, we may think of $J(\mathbf{Q})/[\text{torsion}] \cong P_1 \cdot \mathbb{Z} \oplus P_2 \cdot \mathbb{Z} \oplus \cdots \oplus P_r \cdot \mathbb{Z}$ as giving us a *lattice* (well-defined up to isometry) in Euclidean r-space. Consequently, any isometry-invariant of this lattice is a well-defined invariant of the polarized abelian variety J. The *volume* of the lattice is called the *regulator* of J.

EXAMPLE. S. Deng and G. Call have made computations with the elliptic curve

$$J\colon -206y^2 = x^3 - x^2 + 1/4.$$

[31] Under the hypothesis that the divisor class of the embedding is symmetric.

The three smallest nonzero points in $J(\mathbf{Q})$, the Mordell-Weil group over $\mathbf{Q}$—smallest in the sense of Néron-Tate height—are:

Point	x	y	Néron-Tate Height
P_1	$-15/8$	$7/32$	1.52009244
P_2	$-55/8$	$43/32$	2.05430703
P_3	$-55/98$	$47/1372$	2.42706090

These three points are independent in the Mordell-Weil group, and a descent calculation shows that the Mordell-Weil rank r is $\leqslant 3$. It follows that $r = 3$. Since one also sees that the torsion in $J(\mathbf{Q})$ is trivial, the three "smallest" nonzero points P_1, P_2, P_3 form a basis for the Mordell-Weil group, and also for the canonical lattice (discussed above) in Euclidean three-space. A fundamental domain for this lattice is a parallelopiped with vertices 0, P_1, P_2, P_3 together with the three other points whose x-coordinate and height are given below:

Point	x	Néron-Tate Height
$P_1 + P_2$	$-543/800$	3.51935710
$P_1 + P_3$	$-129/206$	2.82243761
$P_2 + P_3$	$-64287/151250$	6.04387429

The reader can visualize this parallelopiped by imagining cutting and folding the diagram in Figure 15.

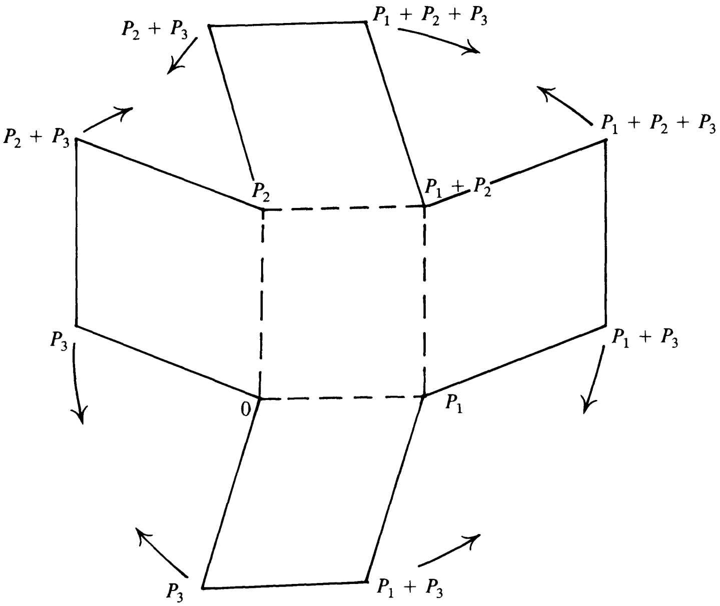


FIGURE 15

For a careful study of another elliptic curve whose Mordell-Weil rank is 3, see [**B-G-Z**].

In our discussion of heights up to this point, we have worked only in $\mathbf{Q}$. More generally, however, we can define a "height function" $h(x)$ for any point $x = (x_0, x_1, \ldots, x_N)$ in $\mathbf{P}^N(K)$ where K is a number field (see, e.g., [**F-W**, p. 34]′ for the standard definition) which coincides with our definition for $N = 2$ and $K = \mathbf{Q}$, which is appropriately calibrated so that $h(x)$ is independent of augmentation of the number field K containing the coefficients of x and which has the all-important finiteness property:

> *For fixed N and K and real number C, there are only a finite number of points x in $\mathbf{P}^N(K)$ such that $h(x) \leqslant C$.*

Similarly, the Néron-Tate height can be defined over any number field K.

If X is a curve of genus $\geqslant 2$ defined over a number field K and imbedded in its jacobian J by an imbedding defined over K, it is a natural question to ask about the "placement" of the rational points $X(K)$ in the lattice in Euclidean r-space determined by the Néron-Tate height. An old theorem of Mumford asserts that if X has genus $g \geqslant 2$ and is imbedded in J in a "normalized" way (cf. [**L2**, p. 120]), then

$$2 \cdot g \cdot \langle x, y \rangle \leqslant |x|^2 + |y|^2 \pm O(1),$$

for $x, y \in X(K)$, $x \neq y$, where $\langle x, y \rangle$ is the Néron-Tate inner product $|x|^2 = \langle x, x \rangle$. An important feature of Mumford's theorem is that the $O(1)$ can be made effective.

Geometrically, the above inequality implies that there cannot be too many points $x \in X(K)$ of roughly the same distance from the origin, and, more specifically, that the number of points of $X(K)$ of distance $\leqslant R$ to the origin is $O(\log R)$.

Although it may seem that Mumford's theorem has been superseded by Faltings, this is not entirely the case (see the discussion in [**Szp 2**, exposé XI, "un peu d'effectivité"]′). Indeed, it is the combination of Mumford's theorem together with Faltings' original techniques (plus extra work) that Parshin and Zarhin suggest as a program to effectively bound the *number* of K-rational points on a curve X of genus $\geqslant 2$ (see Faltings [**F-W**, VI, §6]′).

2. Normed vector spaces. Let us cut a few notational corners by describing this theory in the case where the number field K is the rational field. The generalization to any number field is straightforward.

If $p = 2, 3, 5, \ldots$ is a prime number, recall the *p-adic absolute value* on $\mathbf{Z}$:

$$\|a\|_p = 1/p^n$$

if a is nonzero, where p^n is the highest power of p dividing a. One extends this to $\mathbf{Q}$ by stipulating that $\|0\|_p = 0$ and that the p-adic absolute value be multiplicative. Thus a rational number is small in p-adic absolute value if it is "highly divisible by p".

Letting $\|a\|_\infty = |a|$ denote ordinary absolute value, the *product formula*

$$\prod_v \|a\|_v = 1, \qquad a \in \mathbf{Q} - (0),$$

is immediate (where v ranges through all primes and ∞).

Let W be a vector space of dimension one over $\mathbf{Q}$. To put a *norm* on W is to give functions

$$\| \ \|_v \colon W \to \mathbf{R} \quad (\text{“}v\text{-adic absolute value”})$$

for all v as above, such that:

(i) $\|a \cdot w\|_v = \|a\|_v \cdot \|w\|_v$ for $a \in \mathbf{Q}$, $w \in W$,

(ii) if $w \in W$ is nonzero, then $\|w\|_v = 1$ for all but a finite number of v.

From the product formula one immediately sees that if w is a nontrivial vector in W, then $\prod_v \|w\|_v$ is independent of the choice of w (it depends only on the normed vector space W). Define the *degree* of the normed vector space W to be $-\log \prod_v \|w\|_v$.

Any normed vector space (of dimension one over $\mathbf{Q}$) has a unique pair of vectors $\pm w_0$ such that

$$\|w_0\|_v = 1 \quad \text{for all } v \neq \infty$$

and consequently the subgroup (the ‘lattice’) W_0 generated by w_0 is determined by the norm.

Conversely, the norm on the vector space W is determined by the lattice W_0 together with the single real number $\|w_0\|_\infty$.

Important tautological example. If $\alpha \in \mathbf{P}^2(\mathbf{Q})$ is a point in the projective plane, let $W_\alpha \subseteq \mathbf{Q}^3$ be the line through the origin represented by α. We can put a norm on W_α by taking $W_\alpha \cap \mathbf{Z}^3$ as lattice and defining $\| \ \|_\infty$ to be the logarithm of Euclidean distance in $\mathbf{Q}^3$. One obtains directly from the definitions that

$$h(\alpha) = \operatorname{degree}(W_\alpha).$$

In other words, one can recapture the height of a point by the degree of an appropriate normed vector space.

3. Heights of abelian varieties. Let T be a complex torus of dimension g. So $T \cong \mathbf{C}^g/\Omega$ where Ω is a lattice in complex g space. Let $z_1, \ldots, z_g$ be the linear coordinates on $\mathbf{C}^g$. Then the differential g-form $dz_1 dz_2 \cdots dz_g$ gives rise to an analytic nowhere vanishing differential g-form on T (invariant under translation). Conversely given any everywhere analytic differential g-form ω on T, the ratio of ω by $dz_1 dz_2 \cdots dz_g$ yields an everywhere analytic function on the compact complex analytic manifold T, i.e., a constant.

Summary. Let $D(T)$ denote the complex vector space of everywhere analytic differential g-forms. Then $D(T)$ is one-dimensional over $\mathbf{C}$, generated by $dz_1 dz_2 \cdots dz_g$.

If A is now an abelian variety of dimension g defined over K, there is an algebraic-geometric version of what we have just reviewed for complex tori. One may define *algebraic differential g-forms defined over K*. This forms a one-dimensional vector space over K, denoted $D(A/K)$. If we extend scalars from K to $\mathbf{C}$ we get the space of everywhere analytic differential g-forms on the complex torus $A/\mathbf{C}$.

Example. If $g = 1$, then A (defined over K) has a representation as a cubic plane curve

$$C\colon \varphi(x, y) = y^2 - h(x) = 0,$$

where $h(x)$ is a third degree polynomial with no multiple roots (the origin of A is the unique point at infinity). One easily checks that dx/y has no poles on C, and consequently defines an everywhere analytic differential 1-form. It is a generator of the one-dimensional vector space $D(A/K)$.

When K is a number field, one can do even better: Thanks to a theory of Néron ("*Néron models* of abelian varieties over the rings of integers of number fields") one can make intrinsic sense of the notion of an algebraic differential g-form being *defined over* $\mathcal{O}$, the ring of integers of K. It would lead us too far astray to dwell on this point right now, but the effect of Néron's theory is, for example, when $K = \mathbb{Q}$ to enable us to define a "lattice", i.e., a free abelian subgroup of rank one—the lattice of differential g-forms *defined over* $\mathbb{Z}$—

$$D(A/\mathbb{Z}) \subset D(A/\mathbb{Q})$$

in the one-dimensional vector space $D(A/\mathbb{Q})$.

We can put a canonical *norm* on the one-dimensional vector space $D(A/\mathbb{Q})$ by taking as lattice $D(A/\mathbb{Z})$, and for ω in $D(A/\mathbb{Q})$ we define the ∞-adic absolute value by the integral:

$$\|\omega\|_\infty = \frac{1}{(2\pi)^g}\int_{A(\mathbb{C})} |\omega \wedge \bar{\omega}|.$$

Here $\bar{\omega}$ is the complex conjugate to ω and $\omega \wedge \bar{\omega}$ is therefore a real analytic differential $2g$-form which we integrate over the topological $2g$-manifold $A(\mathbb{C})$.

Summary. To any abelian variety A over $\mathbb{Q}$ we have associated in a canonical manner a *normed vector space* $D(A/\mathbb{Q})$.

DEFINITION. *The raw height* $h(A/\mathbb{Q})$ *of an abelian variety defined over* $\mathbb{Q}$ *is the degree of the normed vector space* $D(A/\mathbb{Q})$.

The theory of raw height makes sense for any number field K. Properly calibrated, it has the property of decreasing under field extension, and remaining unchanged under field extensions L/K provided that the points of A of order 3 (or of order any fixed integer $m \geqslant 3$) are rational over K. It therefore stabilizes. Define the *refined height* of A/K to be the stable raw height:

$$h(A) := \min_{K \subseteq L} h(A/L).$$

The raw height is a good counting function for abelian varieties. Specifically, we have the

FINITENESS PRINCIPLE. *Given*

K: a number field,

g: a natural number,

B: a real number.

Then there are only a finite number of K-isomorphism classes of abelian varieties defined over K, of dimension g, and whose raw height is less than B.

The basic strategy of the proof of the finiteness principle may be divided into three parts:

(1) *Reduction to a finiteness statement for abelian varieties admitting polarizations of degree one and possessing bounded raw height*: This can be done via "Zarhin's trick" (see **[De]**$'$, **[Zar 4]**).[32]

(2) *A study of the moduli space*[33] *of abelian varieties* (*in characteristic zero and of dimension g*) *given with a polarization of degree one.*

For an introduction to that study, see the discussion in **[F-W]**$'$ (especially Chapter 1, and the references cited there). This moduli space is an algebraic variety defined over $\mathbf{Q}$, usually denoted $\mathscr{A}_{g/\mathbf{Q}}$. It is noncompact if $g > 0$, and the various methods used to compactify it are quite intricate. It is of dimension $g(g+1)/2$ (e.g. when $g = 1$, $\mathscr{A}_{g/\mathbf{Q}}$ is the affine line over $\mathbf{Q}$, parametrized by j, the elliptic modular function).

A pair (A, α) where A is an abelian variety of dimension g and α is a polarization of degree one on A defined over K, a field of characteristic zero, gives rise to a well-defined point (call it $J(A, \alpha)$) in the moduli space $\mathscr{A}_g$, rational over K. The point $J(A, \alpha)$ only depends upon the $\overline{K}$-isomorphism class of the pair (A, α).

In **[F-W]**$'$ a specific imbedding of $\mathscr{A}_g$ is given in some high-dimensional projective space over $\mathbf{Q}$. Consequently, we may define, for K a number field, the *height* of a K-rational point of $\mathscr{A}_g$ as being the height in projective space of the image of that K-rational point under this specific imbedding (cf. p. 43 of **[F-W]**$'$).

DEFINITION. *The "moduli-point"*[34] *height of a pair (A, α) defined over a number field K is the height of $J(A, \alpha) \in \mathscr{A}_g(K)$.*

(3) *A comparison of* ***raw height*** *and* ***moduli-point height***. The point is that they don't differ too much (cf. Theorem 3.1 on p. 44 of **[F-W]**$'$). Since there are only a finite number of isomorphism classes (A, α) over K, a fixed number field, with bounded moduli-point height, the finiteness principle follows.

Needless to emphasize, the above three steps only outline the strategy of the proof of the finiteness principle; carrying out that strategy is quite a difficult undertaking.

4. A block diagram. We have gotten to the point where it will be profitable to look ahead at a schematic representation of the whole proof of Mordell's conjecture, even though some of the blocks have not been discussed and some of the terms (*isogeny*, *admissible*[35] *isogeny*, *Tate's conjecture*, *the isogeny conjecture*) have not yet been defined. The format that I am presenting follows Deligne's organization of the proof **[D]**. It owes much, as does Faltings' original presentation, to Zarhin's important work (1974, 1975) on the analogous conjectures over function fields of finite characteristic **[Zar 1, 2, 3]**.

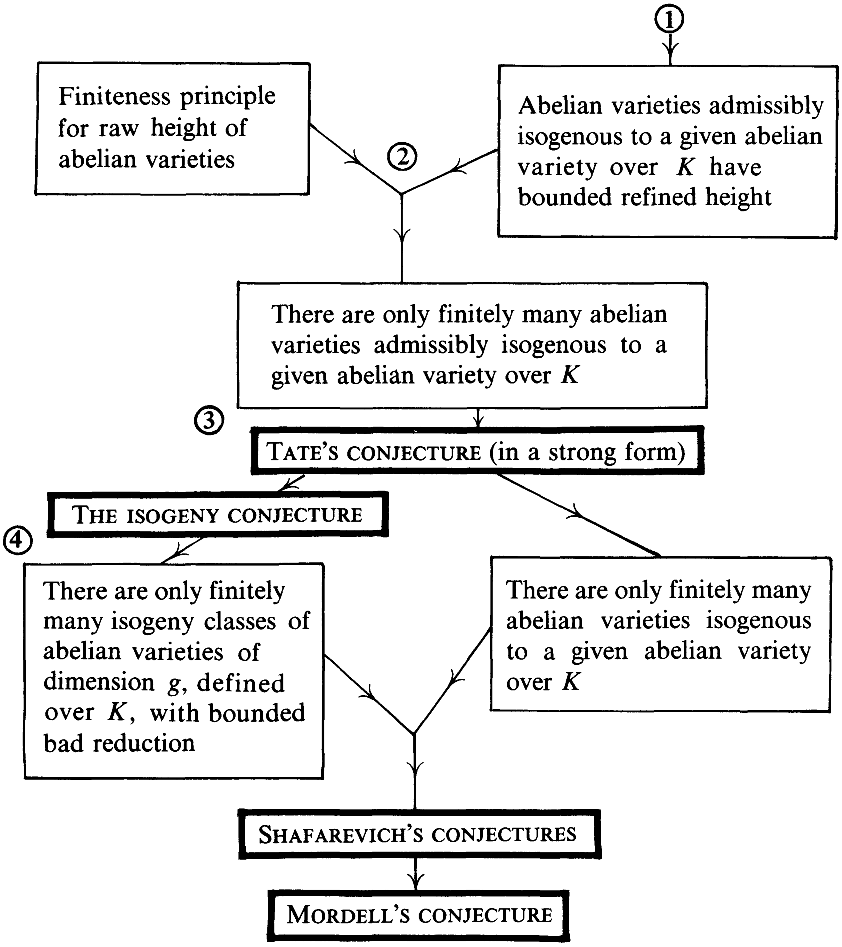
The blocks framed with bold lines represent statements in their final form, while the fine-line framed blocks represent intermediate results. Our field K will be a number field.

[32] This, in general, requires that one's abelian variety be replaced by an abelian variety of 8 times the dimension of the original one.

[33] Technically, it is a "coarse moduli space".

[34] A neologism.

[35] Another neologism.


①
Finiteness principle for raw height of abelian varieties
Abelian varieties admissibly isogenous to a given abelian variety over K have bounded refined height
②
There are only finitely many abelian varieties admissibly isogenous to a given abelian variety over K
③
TATE'S CONJECTURE (in a strong form)
THE ISOGENY CONJECTURE
④
There are only finitely many isogeny classes of abelian varieties of dimension g, defined over K, with bounded bad reduction
There are only finitely many abelian varieties isogenous to a given abelian variety over K
SHAFAREVICH'S CONJECTURES
MORDELL'S CONJECTURE

A homomorphism $f\colon A \to B$ from one complex torus to another is called an *isogeny* if it is surjective and if its kernel is finite. For example, for any complex torus A and any nonzero integer m, multiplication-by-m

$$\text{“}m\text{”}\colon A \to A$$

is an isogeny. Its kernel, denoted $A[m]$, is the group of m-division points in A, a group immediately seen to be isomorphic to

$$(4)\qquad \underbrace{\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \times \cdots \times \mathbb{Z}/m\mathbb{Z}}_{2g \text{ times}} \quad (\text{where } g = \text{dimension of } A).$$

A is said to be *isogenous* to B, if there is such an f. If A and B are abelian varieties defined over K, it makes sense to talk about *isogenies defined over K*. The relation "A is K-isogenous to B" is an equivalence relation.

If A is defined over K, then, for any nonzero integer m, the isogeny "m" of A onto A is defined over K. One can show that the smallest field extension of

K over which each of the m-division points is rational is an algebraic extension of K. If $\bar{K}$ is an algebraic closure of K, one then obtains that each of the points of $A[m]$ (any m) is rational over $\bar{K}$. Any Galois automorphism of $\bar{K}$ over K then acts in a natural way on the group $A[m]$. In this way we get a natural action of $G_K = \mathrm{Gal}(\bar{K}/K)$ on $A[m]$. If you wish, using (4), you may think of this as a representation of G_K into the General Linear Group $\mathbf{GL}_{2g}(\mathbb{Z}/m\mathbb{Z})$. These representations have played and will continue to play an enormously important role in number theory.

Since the Galois action on points of finite order is compatible with the "Weil pairing", a natural nondegenerate skew-symmetric form on $A[m]$, the image of G_K is contained in the subgroup $\mathbf{GSP}_g(\mathbb{Z}/m\mathbb{Z})$ of symplectic similitudes in $\mathbf{GL}_{2g}(\mathbb{Z}/m\mathbb{Z})$.

The case of $g = 1$ has been the focus of attention for a long time. Here $\mathbf{GSP}_1(\mathbb{Z}/m\mathbb{Z}) = \mathbf{GL}_2(\mathbb{Z}/m\mathbb{Z})$. In **[Se 3]** Serre showed that if the elliptic curve A does not have "complex multiplication" i.e., admits no nonscalar endomorphisms, then the index of the image of G_K in $\mathbf{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is bounded by a constant independent of m (depending only on A and K).

Recently (see announcement in **[Se5]**), Serre has shown that if A is an abelian variety of *odd* dimension g not admitting any nonscalar endomorphism and K is a number field, there is a bound b (depending upon K and A) such that if $m = p$ is a prime number greater than b, the representation of G_K into $\mathbf{GSP}_g(\mathbb{Z}/m\mathbb{Z})$ obtained by the action of Galois on $A[m]$ is surjective. In the special case $g = 1$ and $K = \mathbf{Q}$, more is known about the image of G_K. For example, there is a complete determination of the elliptic curves A and integers m such that the image of a conjugate of $G_{\mathbf{Q}}$ in $\mathbf{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is contained in a subgroup of the group of upper-triangular matrices[36] (cf. **[Maz, Ken, Me 3]**).

Given any homomorphism $f\colon A \to B$ of abelian varieties defined over K, one can restrict f to m-division points to get a G_K-equivariant homomorphism (between finite abelian groups)

$$f_m\colon A[m] \to B[m].$$

When does a G_K-equivariant homomorphism

$$\psi\colon A[m] \to B[m]$$

actually come from a homomorphism of complex tori, i.e., when is ψ equal to f_m for some m? One's first instinct, perhaps, is to say: hardly ever! After all, ψ is merely a mapping of finite groups, and why should the G_K-representations on $A[m]$ and $B[m]$ have much bearing on the existence of complex analytic homomorphisms between the tori? Tate conjectured, however, and Faltings has recently proved the following extremely powerful "lifting criterion", which can be "read" in a number of ways to deduce important consequences about abelian varieties, as well as about the G_K-representations to which they give rise:

[36] Equivalently, there is a complete classification of $\mathbf{Q}$-isomorphism classes of isogenies of elliptic curves, defined over $\mathbf{Q}$.

THEOREM (FALTINGS; a version of Tate's conjecture). *Suppose that for each natural number k, the G_K-equivariant homomorphism ψ: $A[m] \to B[m]$ is the restriction of a G_K-equivariant homomorphism $A[m^k] \to B[m^k]$. Then there is a homomorphism of abelian varieties*

$$f\colon A \to B$$

defined over K, such that ψ is the restriction of f to the group of m-division points.

An important consequence, long sought after in its own right, is the closely related "isogeny conjecture".

THEOREM OF FALTINGS (Isogeny conjecture). *Let m be any integer $\geqslant 2$, and A, B abelian varieties defined over a number field K. If there are G_K-equivariant isomorphisms $A[m^k] \to B[m^k]$ for every natural number k, then A and B are isogenous over K.*

We have explained all the terms of the block-diagram except for the technical term *admissible isogeny* which I coined to signal a certain broad class of isogenies which make their appearance in an intermediary stage of the proof. For those who have Deligne's Bourbaki account, I simply mean isogenies satisfying the hypothesis of either his Theorem 2.4 or 2.6. To give some idea of the broadness of this class, for any abelian variety A over K there is an integer M such that any isogeny $A \to B$ defined over K whose kernel has order prime to M is *admissible*; lots of others are, as well.

We conclude our account with a few words about each of the numbered transitions in the block-diagram—signaling some of the mathematical theories which come into play.

(1) This uses Tate's theory of p-divisible groups, some of Raynaud's results concerning finite flat group schemes, and the Weil conjectures for abelian varieties.

(2) What is required here, of course, is some connection between raw and refined heights. It uses the theory of moduli of abelian varieties (cf. exposé IV of **[Szp 3]**).

(3) The strategy of the proof of Tate's conjecture follows, to some extent, Tate's original proof of his conjecture in the context of finite fields, together with some ideas of Zarhin.

In the grossest of terms, Tate's conjecture requires one to construct some K-rational homomorphisms of abelian varieties $A \to B$ under the hypothesis that there are loads of G_K-equivariant homomorphisms of groups of m-division points $A[m] \to B[m]$ (for loads of m's).

There is no loss of generality in supposing that $A = B$, so one is faced with the problem of constructing K-rational endomorphisms of A, under the hypothesis that one has "loads of" G_K-equivariant endomorphisms of groups of m-division points. But given any G_K-equivariant endomorphism of $A[m]$, passing to the quotient of A by the kernel of that endomorphism yields an abelian variety isogenous to A over K. In this manner, by our hypothesis, we obtain an infinite sequence $A_1, A_2, \ldots$ of abelian varieties K-isogenous to A. The first part of the proof of Tate's conjecture uses some elegant algebraic arguments to show, in effect, that one may suppose the A_i are *admissibly* isogenous to A. From the "previous block" in our diagram, there are only a finite number of K-isomorphism classes among all the A_i's. Consequently we get quantities of K-isomorphisms between the A_i's. Composing these isomorphisms with the isogenies connecting the A_i's gives quantities of endomorphisms of various of the A_i's. But these "carry over" to endomorphisms of A itself—precisely the K-endomorphisms that we are required to construct!

(4) The isogeny conjecture assures that the isogeny class of an abelian variety is known once the G_K-representations on m^k-division points are known ($k = 1, 2, \dots$). Faltings uses the Weil conjectures for abelian varieties, together with strong algebraic-number-theoretic implications of "bounded bad reduction" to bound the number of possible systems of G_K-representations in $\mathbf{GL}_{2g}(\mathbf{Z}/m^k\mathbf{Z})$ that may occur. Hence he has also bounded the number of K-isogeny classes.

BIBLIOGRAPHY

1. General references. Here we list works that are accessible, and might be useful, to those who possess no specific background in number theory or algebraic geometry. These are listed roughly in order of relevance to the lectures.

An excellent general history:

[Wl] A. Weil, *Number theory, an approach through history, from Hammurapi to Legendre*, Birkhäuser, Boston, Basel and Stuttgart, 1984.

Introductory texts:

[H-W] G. H. Hardy and E. M. Wright, *The theory of numbers*, 5th ed., Oxford Univ. Press, New York and London, 1979.

[Mo 1] L. J. Mordell, *Diophantine equations*, Academic Press, New York, 1969.

For Pell's equation, there are the works cited above; for specific discussion of the Archimedes Cattle Problem see also:

[Fo] D. H. Fowler, *Archimedes Cattle Problem and the Pocket Calculating Machine*, Preprint, Math. Inst. Univ. of Warwick, Coventry, 1980.

The complete English translation of Viète's treatise:

[Vi 1] François Viète, *Introduction to the analytical art*, in the appendix to J. Klein, Greek Mathematical Thought and the Origin of Algebra, M.I.T. Press, 1968.

[Vi 2] ______, *The analytic art* (transl. T. Richard Witmer), Kent State Univ. Press, 1983.

Hilbert's problems:

[Hi] D. Hilbert, *Mathematical problems*, Lectures delivered before the International Congress of Mathematicians at Paris in 1900; reprinted in *Mathematical developments arising from Hilbert problems*, Proc. Sympos. Pure Math., vol. 28, Amer. Math. Soc., Providence, R.I., 1976, pp. 1–34.

[Da] M. Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly **80** (1973), 233–269.

[D-M-R] M. Davis, Y. Matijasevic and J. Robinson, *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution*, Mathematical Developments Arising from Hilbert Problems, Proc. Sympos. Pure Math., vol. 28, Amer. Math. Soc., Providence, R. I., 1976, pp. 323–378.

An introductory text to elliptic curves which has the *congruent number problem* as its main theme:

[**Ko**] N. Koblitz, *Introduction to elliptic curves and modular forms*, Encyclopedia of Mathematics and its Applications, Addison-Wesley, Reading, Mass., 1984

Added in proof: Another introductory text, which has just appeared:

[–] J. H. Silverman, *The arithmetic of elliptic curves,* Graduate Texts in Mathematics, vol. 106, Springer-Verlag, Berlin, Heidelberg, New York and Tokyo, 1986.

For a discussion concerning the problem of classification of sets of points in the plane with rational distances:

[**Kl**] V. Klee, *Some unsolved problems in plane geometry*, Math. Mag. **52** (1979), 131–145.

[**Mo 2**] L. J. Mordell, *Rational quadrilaterals*, J. London Math. Soc. **35** (1960), 277–282.

A public lecture and audience responses—the subject being Diophantine problems:

[**L 1**] S. Lang, *Une activitė vivante*: *faire des mathématiques*, Rev. Palais de la Découverte **11** (1983), n° 104, 27–62.

An accessible introduction to complex curves; conics, cubics, jacobians:

[**Cl**] C. H. Clemens, *A scrapbook of complex curve theory*, Plenum Press, New York and London, 1980.

A discussion, for nonexperts, of the proof of Mordell's conjecture:

[**Bl**] S. Bloch, *The proof of the Mordell conjecture*, Math. Intelligencer **6** (1984), n° 2, 41–47.

2. References requiring some background. Both of Weil's early papers on the "Mordell-Weil theorem" are readable and enlightening:

[**W 1928**] A. Weil, *L'arithmétique sur les courbes algébriques*, in André Weil, Oeuvres Scientifiques, Collected Papers, vol. I (1926–1951), Springer-Verlag, New York, Heidelberg and Berlin, 1979, pp. 11–46.

[**W 1929**] ______, *Sur un théorème de Mordell*, in André Weil, Oeuvres Scientifiques, Collected Papers, vol. I (1926–1951), Springer-Verlag, New York, Heidelberg and Berlin, 1979, pp. 47–56.

For more on curves:

[**B-K**] E. Brieskorn and H. Knörrer, *Ebene algebraische Kurven*, Birkhäuser, Basel, Boston and Stuttgart, 1981.

[**Mu**] D. Mumford, *Curves and their jacobians*, Univ. of Michigan Press, 1975.

General treatments of background material: Heights, The Mordell-Weil Theorem, Siegel's Theorem, Mumford's Theorem, etc.:

[**L 2**] S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag, New York, Berlin, Heidelberg and Tokyo, 1983.

[**Se 1**] J.-P. Serre, *Autour du théorème de Mordell-Weil*, I & II (Notes of a course given at the Collège de France 1980, edited by M. Waldschmidt), Publ. Math. Univ. Pierre et Marie Curie., 1985.

An expository account of background material specifically used in Faltings' proof, and an account of the proof itself:

[**C-S**] G. Cornell and J. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag (to appear).

A treatment of the theory of quadratic forms:

[**Ca**] J. W. S. Cassels, *Rational quadratic forms*, Academic Press, New York, 1978.

Accounts of the proof of Mordell's conjecture which require familiarity with the techniques of number theory or algebraic geometry. Two expository accounts of the work of Faltings; consult the bibliographies there for further references to the basic papers in the subject:

[De] P. Deligne, *Preuve des conjectures de Tate et Shafarevich* [d'après G. Faltings], Séminaire Bourbaki, exposé n° 616, Novembre 1983.

[Szp 1] L. Szpiro, *La conjecture de Mordell* [d'après G. Faltings], Séminaire Bourbaki, exposé n° 619, Novembre 1983.

The published proof of Mordell's conjecture (for a number field):

[Fa] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

More on Faltings' proof of Mordell's conjecture:

[F-W] G. Faltings, G. Wüstholtz, et al., *Rational points* (Seminar Bonn/Wuppertal 1983/84), Vieweg, Aspects of Mathematics, vol. E6, Braunschweig-Wiesbaden, 1984.

[Szp 2] L. Szpiro, *Séminaire sur les pinceaux arithmétiques*: *La conjecture de Mordell*, Astérisque **127** (1985).

4. Other works cited (alphabetical order):

[A] N. A'Campo, *Sur la première partie du seizième problème de Hilbert* (Séminaire Bourbaki, n° 537, Juin 1979), Lecture Notes in Math., vol. 770, Springer-Verlag, Berlin, Heidelberg and New York, 1980, pp. 208–227.

[A-C-H-P] M. Agrawal, J. Coates, D. Hunt and A. van der Poorten, *Elliptic curves of conductor* 11, Math. Comp. **35** (1980), 259–331.

[Ara] S. J. Arakelov, *Families of algebraic curves with fixed degeneracies*, Izv. Akad. Nauk SSSR Ser. Mat. **35** (1971).

[B-H] J. W. Benham and J. S. Hsia, *Spinor equivalence of quadratic forms*, J. Number Theory **17** (1983), 337–342.

[B-V] E. Bombieri and J. Vaaler, *On Siegel's Lemma*, Invent. Math. **73** (1983), 11–32.

[B-C] A. Bremner and J. W. S. Cassels, *On the equation* $Y^2 = X(X^2 + p)$, Math. Comp. **42** (1984), 257–264.

[B-G-Z] J. Buhler, B. Gross and D. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank* 3, Math. Comp. **44** (1985), 473–481.

[Co] R. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), 765–770.

[de F] Michele de Franchis, *Un teorema sulle involuzioni irrazionali*, Rend. Circ. Mat. Palermo **36** (1913), 368.

[D-R] H. Davenport and K. Roth, *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 160–167.

[Des] M. Deschamps, *Courbes de genre géométrique borné sur une surface de type général* [d'après F. A. Bogomolov] (Séminaire Bourbaki 77/78, n° 519), Lecture Notes in Math., vol. 710, Springer-Verlag, Berlin, Heidelberg and New York, 1979, pp. 233–247.

[Fon] J.-M. Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbf{Z}$, Invent. Math. **81** (1985), 515–538.

[Grau] H. Grauert, *Mordells Vermutung über Punkte auf algebraischen Kurven und Funktionen Körper*, Inst. Hautes Études Sci. Publ. Math. **25** (1965), 363–381.

[Hall] M. Hall, *The diophantine equation* $x^3 - y^3 = k$, Oxford conference, Academic Press, New York, 1971, pp. 173–198.

[Har] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, Berlin, Heidelberg and New York, 1977.

[Hay] T. Hayashida, *A class number associated with the product of an elliptic curve with itself*, J. Math. Soc. Japan. **20** (1968), 26–43.

[Ha-Ni] T. Hayashida and M. Nishi, *Existence of curves of genus two on a product of two elliptic curves*, J. Math. Soc. Japan **17** (1965), 1–16.

[H-S] A. Howard and A. Sommese, *On the theorem of de Franchis*, Ann. Scuola Norm. Sup. Pisa **10** (1983), 429–436.

[Hu] A. Hurwitz, *Über die diophantische Gleichung* $x^3y + y^3z + z^3x = 0$, Math. Ann. **65** (1908), 428–430. Reprinted in *Mathematische Werke* II. Birkhäuser Verlag, Basel-Stuttgart, 1963, pp. 427–429.

[Ken] M. Kenku, *The modular curve* $X_0(39)$ *and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **85** (1979), 21–23.

[Ku] B. Kuhn, *On the canonical Galois closure of the universal elliptic curve over* $X(n)$, Ph.D. thesis, Harvard Univ., 1985.

[L 3] S. Lang, *Integral points on curves*, Inst. Hautes Études Sci. Publ. Math. **6** (1960), 27–43.

[L 4] ______, *Division points on curves*, Ann. Mat. Pura Appl. (4) **70** (1965), 229–234.

[L 5] ______, *Higher dimensional diophantine problems*, Bull. Amer. Math. Soc. **80** (1974), 779–788.

[Man] Y. Manin, *Rational points on algebraic curves over function fields*, Izv. Akad. Nauk SSSR Ser. Mat. **27** (1963). *Beweis eines Analogons der Mordellschen Vermutung für algebraische Kurven über Funktionenkörpern*, Dokl. Akad. Nauk. SSSR **152** (1963), 1061–1063; English transl., Society Mathematics **4** (1963), 1505–1507.

[Ma] R. C. Mason, *On Thue's equation over function fields*, J. London Math. Soc. **24** (1981), 414–426.

[Maz] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[Me 1] J. F. Mestre, *Courbes elliptiques* (Séminaire de Théorie des Nombres, Paris 1981–82), Progress in Math. Series, no. 38, Birkhäuser, Basel, 1983, pp. 179–188.

[Me 2] ______, *Formules explicites et minorations de conducteurs de variétés algébriques* (Thèse Bordeaux, 1984) Compositio Math. (to appear).

[Me 3] ______, *Points rationnels de la courbe modulaire* $X_0(169)$, Ann. Inst. Fourier **30** (1980), 17–27.

[M 2] D. Mumford, *On the equations defining abelian varieties*. I, II, III, Invent. Math. **1** (1966), 287–354; **3** (1967), 75–135; **3** (1967), 215–244.

[M 3] ______, *Abelian varieties*, **5**, Tata Inst. Fund. Research. Studies in Math., Oxford Univ. Press, 1970.

[Na-No] M. S. Narasimhan and M. V. Nori, *Polarizations on an abelian variety*, Proc. Indian Academy of Sciences **90** (1981), 125–128.

[No] J. Noguchi, *A higher dimensional analogue of Mordell's conjecture over function fields*, Math. Ann. **158** (1981), 207–212.

[Par 1] A. N. Parshin, *Algebraic curves over function fields*. I, Izv. Akad. Nauk SSSR Ser. Mat. **32** (1968), no. 5, 1145–1170.

[Par 2] ______, *Quelques conjectures de finitude en géometrie diophantienne*, Actes Congr. Internat. Math. **1** (1970), 467–471.

[Se 2] J.-P. Serre, *Courbes elliptiques de conducteur* 11, Lectures delivered at the College de France 1984/85.

[Se 3] ______, *Propriété galoisienne des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[Se 4] ______, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968.

[Se 5] ______, *Résumé des cours de* 1984–1985, Annuaire du Collège de France, 1985.

[Sev] Francesco Severi, *Sugli integrali abeliani riducibili*, Rend. Accad. Lincei Ser. V **23** (1914), 581–587.

[Shaf] I. R. Shafarevich, *Algebraic number fields*, Proc. Internat. Congr. Math., Stockholm 1962, Institute Mittag-Liffler, Aljursholm, 1963, pp. 163–176; English transl., Amer. Math. Soc. Transl. (2) **31** (1963), 25–39.

[Si] J. H. Silverman, *Representations of integers by binary forms and the rank of the Mordell-Weil group*, Invent. Math. **74** (1983), 281–292.

[Szp 3] L. Szpiro, et al., *Séminaire sur les pinceaux de courbes de genre au moins deux*, Astérisque **86** (1981).

[Ta] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Math., 1962, pp. 288–295.

[Vo] P. Vojta, *A higher dimensional Mordell conjecture*, Preprint, Yale, 1984. Also: *Diophantine approximation and value distribution theory*, Preprint, Yale, 1985.

[Weyl] H. Weyl, *Algebraic theory of numbers*, Ann. of Math. Studies, no. 1, Princeton Univ. Press, Princeton, N. J., 1940.

[Zar 1] J. G. Zarhin, *Isogenies of abelian varieties over fields of finite characteristic*, Mat. Sb. **95** (**137**) (1974), no. 3, 451–461.

[Zar 2] ______, *A remark on endomorphisms of abelian varieties over function fields of finite characteristic*, Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974), no. 3, 477–480.

[Zar 3] ______, *Finiteness theorem for isogenies of abelian varieties over function fields of finite characteristic*, Funktsional. Anal. i Prilozhen. **8** (1974), no. 4, 31–34.

[Zar 4] ______, *A finiteness theorem for unpolarized Abelian varieties over number fields with prescribed places of bad reduction*, Invent. Math. **79** (1985), 309–321.

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MASSACHUSETTS 02138