In 1983 Faltings proved conjectures by Mordell, Shafarevich and Tate.

Frans Oort
Mathematisch Instituut
Budapestlaan 6
3508 TA Utrecht
The Netherlands

Introduction

In a rather short paper [F] we find proofs of several striking and deep theorems. Admiring experts are said to call the result by G. Faltings which confirms the Mordell conjecture 'the theorem of the century' (cf. John Ewing's 'Editorial' in *The Math. Intelligencer*, *5* (1983), number 4).

Already several expository papers have been devoted to these results; in [Fa3] we find a survey for non-specialists by G. Faltings; in the Bourbaki talks [D] and [S] several details of the proof are carefully examined; newspapers all over the world have reported on these achievements; several specialists study these theorems, the proofs and further developments. It may be hoped that *Séminaire Szpiro* 1983/1984 will appear in print and it seems that A.N. Parshin is planning to write a survey article on this material. Hence there is no need for any exposition of these kinds; therefore, in this note, we restrict ourselves to stating the theorems and to making some side-remarks on their significance.

1. Hilbert's tenth problem

In Paris, at the International Congres of Mathematicians, 1900, David Hilbert delivered a lecture, in which he posed 23 problems. The 10th reads:

> '*10 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.'

Excellent surveys of developments arising from the Hilbert problems can be found in the 2 volumes of [Proc.]. In 1970 MATIJASEVICH gave a negative answer to the tenth problem. Thus we are faced with the reality that in treating diophantine equations ad hoc methods will be needed; a fact which mathematicians can digest only with some difficulty. However,

> 'One of the charms of mathematics is the constant discovery of unexpected almost unbelievable connections. Whatever is logically possible may be true!' (cf. [Proc.], part 2, p.338).

Thus, the systematic approach Hilbert was asking for does not exist, but mathematics seems in this way to gain interest instead of loosing it.

2. A theorem and a conjecture by Mordell

Let us consider one equation in two variables, and try to find rational solutions. For example:

$$X^2+Y^2 = 1; \tag{1}$$

we see immediately that for any $t \in \mathbf{Q}$,

$$x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2}$$

is a solution (also $(-1,0)$ is a solution, and in this way we obtain all of them). Thus we see that the equation has infinitely many solutions with $x,y \in \mathbf{Q}$. For cubic equations the situation is already much more complicated. Consider:

$$Y^2 = X^2(X-1) \tag{2}$$

$$Y^2+Y = X^3-X \tag{3}$$

$$X^3+Y^3 = 1 \qquad (4);$$

the equation (2) has infinitely many rational solutions (and it is easy to find them all: with the help of lines through the singularity (0,0) we can parametrize the curve rationally, as we did in the previous case); the equation (3) has many solutions over $\mathbf{Q}$, for example

$$x = \frac{21}{25}, \quad y = \frac{-56}{125}$$

is a solution of (3), but it is not so easy to find all solutions; of course, equation (4) has no solutions (x,y) with $xy \neq 0$. We see the difficulties, and, what happens if we consider equations of higher degree?

To an algebraic rational curve C one can attach a natural invariant, the *genus*, $g(C)$. This non-negative integer can be defined in several ways. For example, it can be given with the help of the topology on the set of complex points of C, i.e. with the Riemann surface $C(\mathbf{C})$. If C is a curve in the projective plane $\mathbf{P}^2$, given by an equation involving an irreducible polynomial of degree n, then

$$g(C) \leqslant \tfrac{1}{2}(n-1)(n-2)$$

and equality holds iff C is a *smooth curve* (this means that it has no singularities over $\mathbb{C}$). The curves in (1), (2), (3), (4) have genus 0,0,1,1, respectively. Note the remarkable twist: we started studying a purely algebraically given equation, we see that equations which look alike may be different in behaviour, and the difference will be (partly) explained by properties of a topologic/geometric concept such as a Riemann surface (working over $\mathbb{Q}$, we use the topology of the Riemann surface of points with coordinates in $\mathbb{C}$). This combination of arithmetic and geometry will be used to study the question:

given $f \in \mathbb{Q}[X,Y]$, find solutions:

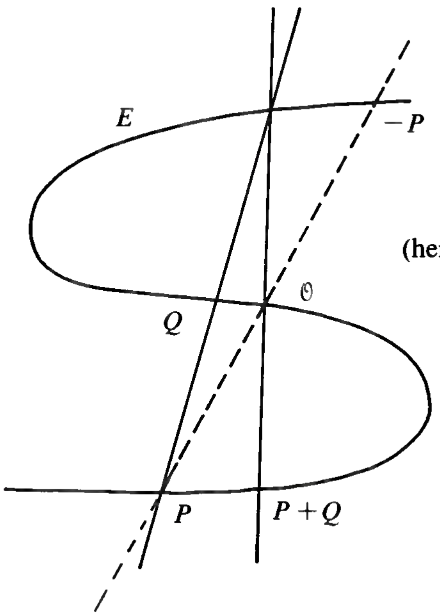
$x,y \in \mathbb{Q}$ or $x,y \in \mathbb{Z}$, with $f(x,y) = 0$.

From now on C is the complete curve given by such a polynomial f.

For *rational curves* (i.e. those with $g(C)=0$) the set $C(\mathbb{Q})$ of solutions $x,y \in \mathbb{Q}$ is easily described:

either there are no solutions (e.g. $X^2+Y^2=-1$),
or there are infinitely many solutions (use a parametrization).

However solutions $x,y \in \mathbb{Z}$ are much more difficult. We come back to this question later.



(here $\mathcal{O}$ is a flex of $E \subset \mathbb{P}^2$)

If $g(C)=1$, we say we have an *elliptic curve* (the name: computing the arc-length of an ellipse, WALLIS 1655, led to *elliptic integrals*, e.g. studied by LEGENDRE 1825, and these functions parametrize curves with $g=1$, WEIERSTRASS 1825; therefore curves with $g=1$ are called elliptic curves). Any curve with $g(C)=1$, and $C(\mathbf{Q})\neq\varnothing$ can be given by a cubic equation (and for a cubic polynomial f, the curve has either $g(C)=0$ if it is singular, or $g(C)=1$ if it is smooth). If E is elliptic, $E\subset\mathbf{P}^2$, and it has a rational point, then its set of points forms a commutative group, in a very natural way (use a geometric description of this group law, or use the addition theorem for the Weierstrass $\wp$-function). For an elliptic curve MORDELL proved in 1922:

let E be an elliptic curve; the group $E(\mathbf{Q})$ is *finitely generated*

(cf. [Mo1]); hence

$$E(\mathbf{Q})\simeq\mathbf{Z}^r\oplus T,$$

with $r\in\mathbf{Z}_{\geqslant 0}$ and T a finite commutative group, $T=\text{Tors}(E(\mathbf{Q}))$, the torsion subgroup of $E(\mathbf{Q})$. This theorem can be generalized, as A. WEIL proved: for any abelian variety A over a number field K (i.e. $[K:\mathbf{Q}]<\infty$), the group $A(K)$ is finitely generated (cf. [We1]). These results did not end this subject, but rather started fascinating research areas, such as computation of r and T for a given E. Some deep results have been achieved (such as: for any E,

$$\#T\leqslant 16,$$

where $T=\text{Tors}(E(\mathbf{Q}))$, MAZUR, 1976, cf. [Maz]), but many questions remain open (Birch and Swinnerton-Dyer conjecture; Taniyama and Weil conjecture, and many other difficult problems; an adequate description would lead us much too far). Thus the 1922 result by MORDELL started a wide field of research. At the same time MORDELL formulated a conjecture (which, by FALTINGS, is now a theorem):

(M). *Let K be a number (i.e. K is a finite extension of $\mathbf{Q}$), let C be an algebraic curve over K, assume $g(C)\geqslant 2$, then $\#(C(K))<\infty$.*

Note, as a corollary:

Let $n\in\mathbf{Z}_{\geqslant 3}$, then $\#\{x,y\in\mathbf{Q}\mid x^n+y^n=1\}<\infty$

because the projective curve defined by the homogeneous equation $X^n+Y^n=Z^n$ has no singularities, hence its genus equals $g=\frac{1}{2}(n-1)(n-2)$, and $n\geqslant 4$ implies $g\geqslant 3$, while for $n=3$ we already know the result to be true.

Fermat's 'last theorem' would say there are no rational solutions of this equation with $xy\neq 0$.

3. Questions and conjectures

An open problem in mathematics can be very stimulating. Whole branches of this discipline have been developed in order to settle a certain question. Sometimes it seems that answering a question makes the field less interesting. In some cases the methods turn out to be of greater importance than the results aimed at. It also happens that the new theorems open new fields, give new impetus to further research.

I think these results by FALTINGS will trigger new ideas. In itself the fact that the Mordell conjecture has been solved is perhaps not so far-reaching, but it gives a certainty that mathematical reality has such nice aspects, and, even more importantly, the method of proof, and in particular the validity of conjectures by SHAFAREVICH and by TATE (cf. below) is of great technical importance.

When do we, mathematicians, say that a certain idea or hope is a conjecture? Well, there seem to be different tastes. Let me illustrate this with two examples. In 1955 SERRE posed a question, cf. [FAC], page 243 (is every finite type projective $K[X_1, \ldots, X_n]$-module free?). Soon several mathematicians called this the Serre conjecture (it has been solved affirmatively), but to me it seemed to be more in the style of the author in question to refer to this as 'a question posed by SERRE' or 'the Serre problem'. I remember a discussion between SERRE and LANG, Arcata, 1974, where SERRE in his talk formulated a certain question. LANG, in the audience, thought that enough numerical evidence was available to have that question given the status of a conjecture, while SERRE remained resistent to do so.

So, we see that different mathematicians may have different opinions about the meaning of the word 'conjecture'. We cite A. WEIL from his commentary [We4], Vol. III, pp. 453/454:

> '... j'évitai de parler de "conjectures". Ceci me donne l'occasion de dire mon sentiment sur ce mot dont on a tant usé et abusé.
>
> Sans cesse le mathématicien se dit: "Ce serait bien beau" (ou: "Ce serait bien commode") si telle ou telle chose était vraie. Parfois il le vérifie sans trop de peine; d'autres fois il ne tarde pas à se détromper. Si son intuition a résisté quelque temps à ses efforts, il tend à parler de "conjecture", même si la chose a peu d'importance en soi. Le plus souvent c'est prématuré.
>
> En théorie des groupes, on a longtemps parlé d'une "conjecture de Burnside", qu'à vrai dire celui-ci, fort judicieusement, n'avait proposée que comme problème. Il n'y avait pas la moindre raison de croire que l'énoncé en question fût vrai. Finalement il était faux.
>
> Nous sommes moins avancés à l'égard de la "conjecture de Mordell". Il s'agit là d'une question qu'un arithméticien ne peut guère manquer de se poser; on n'aperçoit d'ailleurs aucun motif sérieux de parier pour ou contre. Peut-être dira-t-on que l'existence d'une infinité de solutions rationnelles pour une

équation $f(x,y)=0$, en l'absence d'une raison algébrique qui la justifie, est infiniment peu probable. Mais ce n'est pas un argument ...

En ce qui concerne les questions posées à la fin de [1967a], tant de résultats partiels sont venus depuis lors s'ajouter aux miens qu'à présent je n'hésiterais plus, je crois, à parler de "conjectures", encore que le terme d'"hypothèse de travail" soit peut-être plus approprié. En tout cas, s'il m'appartenait de donner un conseil à qui ne m'en demande point, je recommanderais d'employer désormais le mot de "conjecture" avec un peu plus de circonspection que dans ces derniers temps.'

Of course the fact that a question turns out to have an affirmative answer does not justify afterwards having used the terminology 'conjecture', thus I have reproduced the opinions by SERRE and WEIL.

4. INTEGRAL POINTS: THE SIEGEL THEOREM

We like to study integral solutions of equations. Let me give a warning at this point. Previously in this note we have gone back and forth between a polynomial F and the algebraic curve defined by the equation $F=0$. But of course, in studying integral solutions, the isomorphisms of the curves must be taken over the ring of integers. Let me illustrate this with an example. The curves defined by

$$Y^2+Y = X^3-X \quad \text{and} \quad \eta^2+8\eta = \xi^3-16\xi$$

are isomorphic over $\mathbf{Q}$ (by $4X=\xi$, $8Y=\eta$), they are not isomorphic over $\mathbf{Z}$, the point $(\xi=1, \eta=-5)$ is an integral solution of the second equation but the corresponding $\mathbf{Q}$-rational point $(x=\frac{1}{4}, y=-\frac{5}{8})$ does not have integral coordinates. This shows we have to be careful in saying something like 'an integral point on a curve over $\mathbf{Q}$'.

The following *theorem* should be called the Thue-Siegel-Mahler *theorem on integral points* on curves over number fields.

(S). *Let K be a number field, let S be a finite set of discrete valuations of K, and let*

$$R = R_S := \bigcap_{v \notin S} \mathcal{O}_v$$

(the ring of elements of K, integral outside S). Let $\mathcal{C}$ be a smooth affine algebraic curve defined over R. Assume, either

a) $g>0$ *(here g is the genus of the compactification $\overline{C}$ of $\mathcal{C}\otimes_R K$); or*

b) $g=0$ *and* $\#(\overline{C}(\overline{K})-C(\overline{K}))\geq 3$.

Then

$$\#\,\mathcal{C}(R) < \infty$$

(cf. [La3] for references).

Example. Let $K = \mathbf{Q}$, $S = \varnothing$, $R = \mathbf{Z}$, and suppose C is given by the equation $Y^2 = X^3 + 17$. If v is a discrete valuation corresponding to the prime p then $\mathcal{O}_v$ consists of all elements that can be written as a/b with $a \in \mathbf{Z}$, $b \in \mathbf{Z}$ and $\gcd(b,p) = 1$. Thus $R_S = R$. The curve $\mathcal{C}$ is smooth and $g(\mathcal{C}) = 1$, so the equation $Y^2 = X^3 + 17$ has finitely many integral solutions by the above theorem (and NAGELL determined all of them, cf. [Mo2], page 246).

Application. Let K, S, R be as above. It is known that R^* (the group of units of R) is finitely generated. We write

$$J_{K,S} := R^* \cap (1 + R^*) =$$
$$= \{\lambda \in R \mid \lambda \in R^* \quad \text{and} \quad (\lambda - 1) \in R^*\}.$$

Applying (S) with $\mathcal{C}$ the curve given by the complex projective line minus three points $\mathbb{P}^1 - \{0, 1, \infty\}$, we get

$$\# J_{K,S} < \infty$$

(cf. [Ch]; this was known as a conjecture of JULIA ROBINSON).

Theorem (S) with $R = \mathcal{O}(K)$, i.e. $S = \varnothing$, was known in 1929. The proof was not easy. Through the work of FALTINGS we obtain a new proof (with S finite, arbitrary).

It would be more systematic to put the theorem in the following form: K, S, R as above, $\mathcal{C}$ an algebraic smooth curve defined over R, $\bar{C}$ the compactification of $\mathcal{C} \otimes_R K$. Then $\mathcal{C}(R)$ is finite in each of the following cases:

(0) $g = 0$, $\#(\bar{C}(\bar{K}) - C(\bar{K})) \geqslant 3$;
(1) $g = 1$, $\#(\bar{C}(\bar{K}) - C(\bar{K})) \geqslant 1$;
($\geqslant$2) $g \geqslant 2$ (the Mordell case).

In this form the theorem becomes much more natural (to me) than in the classical form. The numbers 3 (for $g = 0$), 1 (for $g = 1$) and 0 (for $g \geqslant 2$) are the numbers of zeros which imposed on a global vector field on such a curve makes it constant. This is what naturally comes out of the arithmetic-geometric proof of (S).

So far we have described mathematical ideas and theorems mainly developed between 1900 and 1930. To prove something like the Mordell conjecture it turned out that new techniques were necessary. It took mathematicians a long time to develop these new methods. As FALTINGS pointed out on several occasions, his achievements were possible after much work done by SHAFAREVICH, TATE, MUMFORD, PARSHIN, ARAKELOV, ZARHIN, RAYNAUD and many others. The way FALTINGS combines these ideas is certainly astonishing, and in his proof several ingenious turns can be seen. But we like to point out the importance of previous developments. Also we like to stress again the influential role of algebraic geometry:

> 'Allgemein läszt sich sagen, dasz die Beweismethoden aus der algebraischen Geometrie stammen... Es scheint jedoch, als ob die Tragweite dieser Entwicklungen von vielen Zahlentheoretikern nicht voll erkannt worden ist. Es zeigt sich hier einmal mehr, dasz die Zahlentheorie zwar zu Recht die Königin der Mathematik genannt wird, sie aber ihren Glanz, wie auch Königinnen sonst, nicht so sehr aus sich selbst als viel mehr aus den Kräften ihrer Untertanen zieht.' (FALTINGS, [Fa3], p. 1).

Or, we can read in [We5] on page 405 the way in which WEIL considers the relationship between the theory of diophantine equations and algebraic geometry:

> '... après de timides essais de Hilbert et Hurwitz, puis de Poincaré, Mordell remit les equations diophantiennes en honneur en demontrant son célèbre théorème, apres quoi l'analyse de Diophante est devenue une branche, et non des moindres, de la géométrie algébrique. Les rôles se sont renversés. A present la mère a élu domicile chez sa fille.'

5. THE SHAFAREVICH PHILOSOPHY

In Stockholm, at the International Congress of Mathematicians, 1962, I.R. SHAFAREVICH discussed certain finiteness conjectures. His philosophy reads as follows:

a) fix a base B (e.g. the arithmetic case: K is a number field and S a finite set of discrete valuations of K, then B is the set $\mathrm{Spec}(R_S)$ of all prime ideals of R_S; or the function field case: let B be some algebraic variety);

b) consider certain objects defined over the base (field extensions of K, algebraic curves over K, abelian varieties over K,...; these objects may have some extra structure);

c) fix discrete invariants of these objects and insist on 'good behaviour' of these objects with respect to the base (such as properties of *non-ramification*, or of *good reduction* outside S).

We denote the set of objects satisfying such data by

$$\mathrm{Sh}((a);(b);(c)).$$

Often, reference to 'good behaviour' will be suppressed in (c). The Shafarevich philosophy is that in certain cases one may hope that

$$\# \mathrm{Sh}((a);(b);(c)) < \infty.$$

Example (Theorem of Hermite). Fix a number field K and a set S of discrete valuations of K with $\#S<\infty$; fix $n \in \mathbb{Z}_{\geq 1}$ and consider field extensions $L \supset K$ of degree $[L:K]=n$, such that L is unramified K outside S. Then

$$\# \operatorname{Sh}(K,S;\ \text{fields } L;\ [L:K]=n) < \infty$$

(here the objects of course are considered up to $\simeq$ over K) (cf. [Ha], p.595).

This is the first example of the Shafarevich philosophy; one could say that this is the case of 'relative dimension zero', and n is the other discrete invariant we fix. To formulate the ideas by Shafarevich we generalize the notion of 'unramified' in the case of algebraic varieties over a field with a discrete valuation.

Let K be a field, v a discrete valuation of K, and $R_v \subset K$ its valuation ring. Let C be a complete curve over K. We say that C has *good reduction* at v if there exists a smooth, proper curve C defined over R_v such that $\mathcal{C} \otimes_{R_v} K \simeq C$. As an example, let E be the projective plane curve given by the equation

$$Y^2Z = X^3+5^6Z^3.$$

This equation can be used to define a curve over $\mathbb{Z}$, but at the prime 5 this equation defines a singular curve. However E has good reduction at the prime 5, because over $\mathbb{Q}$ it can also be defined by the equation

$$\eta^2\zeta = \xi^3+\zeta^3$$

($Y=5^3\eta$, $X=5^2\xi$, $Z=\zeta$), and this new equation defines a curve over $\mathbb{Z}$ which at the prime 5 has a smooth fibre. There is a lot of literature on this subject, but we shall leave this aside.

Example. SHAFAREVICH proved: Fix K, S, $g \geq 1$, then

$$\# \operatorname{Sh}(K,S;\ \text{(hyper)elliptic curves } C;\ g(C)=g) < \infty$$

(cf. [Se4], p. IV-7, [Pa3], p.79 and [Oo6], Th. 3.1 for details and proofs).

These proofs depend on the Siegel theorem (S). By FALTINGS we now have a proof independent of (S).

We can also study these questions for abelian varieties (over number fields, etc.). In this case definitions of good reduction can be given which are analogous to those for curves. The *Shafarevich conjecture* (now a theorem by FALTINGS) reads:

(Sh). *Let K be a number field and let S be a finite set of discrete valuations of K, fix $g \in \mathbb{Z}_{\geq 1}$; the set of abelian varieties of dimension g, defined over K, having good reduction for every $v \notin S$ (up to isomorphism over K) is a finite set:*

$$\# \operatorname{Sh}(K,S;\ \textit{abelian varieties } A;\ \dim(A)=g) < \infty.$$

Remark. In some formulations of this conjecture it seems easier to use *polarized* abelian varieties. A trick by ZARHIN tells us that for any abelian variety A the abelian variety $A^4 \times (A^t)^4$ has a principal polarization. So, if we can prove (Sh) for *all* g in the principally polarized case, the conjecture follows for abelian varieties. In the arithmetic case this simplification can be made; in the function field case there are some difficulties.

Example. Take $K = \mathbf{Q}$, $S = \varnothing$. It seems to be true that

$$\mathrm{Sh}(\mathbf{Q}, \varnothing; \text{abelian varieties } A; \dim(A) = g) = \varnothing$$

for every g. For $g=1$ this is due to TATE (cf. [Ogg], p.145); this is a special case of the Taniyama-Weil conjecture. For $g \leqslant 3$ this was proved by ABRASHKIN, cf. [Ab]. I was just informed (July 1984) that RAYNAUD has proved this for all g.

Let C be an algebraic curve (over K), and $A = \mathrm{Jac}(C)$ its Jacobian variety. If C has good reduction at v, then A has good reduction at v (the converse is false). Therefore, from (Sh) we can easily derive:
(Sh, curves). Let K, S, g be as before, then

$$\# \mathrm{Sh}(K, S; \text{curves } C; g(\mathcal{C}) = g) < \infty.$$

6. THE IMPLICATIONS (Sh) ⇒ (M), AND (Sh) ⇒ (S)

In 1967, KODAIRA constructed certain surfaces as branched coverings of another surface (cf. [Ko]; cf. [Ka]). His construction can be performed in a purely algebraic context, and it can also be applied to $\mathcal{C}$, where C is an algebraic curve over K, further $R \subset K$ and $\mathcal{C} \to Spec(R)$ (note that the (Krull-) dimension of $\mathcal{C}$ equals 2, there is the analogy). In this way PARSHIN showed that the Mordell conjecture would follow from the Shafarevich finiteness statement for curves (cf. [Pa1], p.1168, Remark 2; cf. [Pa2]). We sketch the arguments. Suppose there is given a curve C over K, and $g(C) = g \geqslant 2$; we want to show

$$\# C(K) < \infty.$$

Choose an even positive integer q (e.g. $q=2$), and construct for every $P \in \mathcal{C}(K)$ the following objects: an étale covering $C_1 \to C$ by pulling back $q \cdot id_J$ (where $J = \mathrm{Jac}(C)$);

$$\begin{array}{cccc} & C_1 & \to & J & \\ f & \downarrow & & \downarrow & q \\ & C & \to & J, & \end{array}$$

a divisor δ_P on C_1 by

$$\delta_P = f^*(P)$$

(note that C_1 is an irreducible algebraic curve defined over K); note that $\deg(\delta_P) = q^{2g}$, so it is even. Let K_P' be the smallest field for which there exists a divisor δ_P' on C_1, rational over K_P', such that

$$\delta_P \sim 2\delta_P'$$

(linear equivalence over K_P' on C_1). Now use the Kodaira construction: there exists an algebraic curve C_P and a 2:1-covering

$$C_P \to C'$$

which ramifies exactly at δ_P (proof: if δ_P is locally given by $f \in \Gamma(U,\mathcal{O})$, where $U \subset C_1$ is affine open, then C_P is locally given by

$$\mathrm{Spec}(\Gamma(U,\mathcal{O})[T]/(T^2-f)),$$

and $\delta_P \sim 2\delta_P'$ tells us that these open pieces glue to a scheme over K_P'). Note that $g(C_P)=:h$ is determined by g and q (use the Hurwitz formula for the coverings $C' \to C$ and $C_P \to C'$). There exists a field L such that $[L:K]<\infty$, with $L \supset K_P'$, for all $P \in C(K)$. This fact is crucial; it follows from the theorem of Hermite: take K_P' inside the field of rationality for the points of the fibre above $[\delta_P]$ in

$$\times 2: \underline{Pic}^m(C_1) \to \underline{Pic}^{2m}(C_1), \quad m = q^{2g};$$

this bounds the degree of K_P' and K_P'/K is unramified for all discrete valuations v with $v|2$ and such that C has good reduction at v.

Now let T be the set of all discrete valuations w of L with the property that $w \dagger 2$ or there exists a valuation v on K, satisfying $w|v$ such that C has bad reduction at v. Clearly $\#T<\infty$. Furthermore C_P has good reduction for all $w \notin T$ (this follows by extending the coverings $C_P \to C' \to C$ to $\mathrm{Spec}(R_w)$). Thus we arrive at a map:

$$P \mapsto C_P$$

$$C(K) \to \mathrm{Sh}(L,T;\ \text{curves } C;\ g(C)=h).$$

As said before, once K, C, q are given, then L, T and h are fixed. We show that the fibres of this map are finite. From the covering $C_P \to C$ we can find back the point P (because this map ramifies exactly at $P \in C$). Therefore the claim follows from the following observation:

> let D and C be curves, $g(C) \geqslant 2$, then the set of separable surjective maps from D to C is finite

(there are many ways of proving this, e.g. it is a special case of the theorem of De Franchis, cf. [La3], or, use [Oo5] p.111, Lemma 3.3.; thus

$$\#\,\mathrm{Sh}(L,T;\ \text{curves } C;\ g(C)=h) < \infty$$

implies

$$\#C(K) < \infty,$$

which is the sought-for finiteness statement in the Mordell conjecture. So far for the implication (Sh)$\Rightarrow$(M).

In order to derive (S) from (Sh) we consider C over K with $Q \in C(K)$ (case $g(C)=1$), respectively $Q_0, Q_1, Q_2 \in C(K)$, 3 different points ($g(C)=0$). Let S be a finite set of discrete valuations of K, let $R=R_s$ be as before, and let $\mathcal{C} \rightarrow \mathrm{Spec}(R)=B$ be a curve obtained by extending C over B, and omitting the section extending Q (we describe only the case $g(C)=1$). For any $P \in \mathcal{C}(R)$ (i.e. $P \in C(K)$ such that for each $v \notin S$ the sections extending P and Q do not intersect above v) we take

$$f = \times q : C \rightarrow C$$

and we define

$$\delta_P = f^*(P+Q);$$

from here we proceed as before. In case $g(C)=0$, for any $P \in \mathcal{C}(R)$ we choose $E_P \rightarrow C$, 2:1, ramified exactly at P, Q_0, Q_1 and Q_2, and we continue as before. In particular, the observation:

> let D and E be curves, $g(E)=1$, let $Q \in E$, the set of separable surjective maps from D to E which ramify at Q is finite

(and the analogous statement for $g(C)=0$ and $Q_0, Q_1, Q_2 \in E$) can be used to finish the proof.

We see that this geometric approach to arithmetic problems is very strong. It brings out clearly what the correct conditions should be. These finiteness theorems are exactly the kind of problems which can be handled in this way.

However these methods also have limitations. Note that in order to study an 'easy' equation like $X^n + Y^n = Z^n$ over an 'easy' field like $\mathbf{Q}$, the geometric method has to work via a large extension of $\mathbf{Q}$, and the proof uses geometric objects (abelian varieties) for which it is almost impossible to write out simple defining equations. Thus for mathematicians who like to work with explicitly given formulas these ideas seem far away from more 'concrete methods'. This solution of (M) does not belong to what we call 'elementary methods' in number theory (some elementary methods are very difficult!). The reader could see the discussion between MORDELL and LANG as recorded in [La3], pp. 349–358. We hope that the various developments have a positive mutual influence.

We note that (at the moment) the geometric method does not give effective bounds. (We would like to produce for each equation a bound for the coordinates of the solutions). It seems that RAYNAUD and PARSHIN can give a bound for the *number* of the solutions of the Fermat equation $X^n + Y^n = Z^n$, $n \geqslant 3$, with $x, y, z \in \mathbf{Z}$ and coprime. Using the 'effective Chebotarev', cf. [LMO], part of the proof by FALTINGS can be made effective.

7. The Tate conjecture

In order to handle (co)homology of an algebraic curve C it is very useful to know properties of the abelian variety $\mathrm{Jac}(C)$. Thus one is naturally led to the study of abelian varieties. We denote for any $n \in \mathbf{Z}_{\geqslant 1}$ by $A[n]$ the kernel of the map

$$n.id_A : A \to A$$

(here A is an abelian variety). If A is defined over a field M, and $\mathrm{char}(M)$ does not divide n, then

$$A[n](\overline{M}) \simeq (\mathbf{Z}/n)^{2g}, \quad g = \dim A$$

(this is easy if $\mathrm{char}(M)=0$, once you know that

$$A(\mathbf{C}) \simeq \mathbf{C}^g / \Lambda,$$

where $\Lambda \simeq \mathbf{Z}^{2g}$ is a lattice in $\mathbf{C}^g$). For a prime number l we denote by

$$T_l A = \varprojlim_i A[l^i](\overline{M})$$

(projective limit taken with respect to $\times l : A[l^{i+1}] \to A[l^i]$). This is an abelian group,

$$T_l A \simeq (\mathbf{Z}_l)^{2g},$$

and Gal (M^s/M) acts on it in a continuous way, here M^s denotes the separable closure of M. The advantage of these concepts is that they can be studied over any base, and that they make visible a lot of the structure you want to study. If A and B are abelian varieties over a field M we like to determine $\mathrm{Hom}_M(A,B)$ (for example, given $E=A$, and $E'=B$ are elliptic curves over $\mathbf{Q}$, say such that $E \bmod p$ and $E' \bmod p$ are isogenous for (almost) all p, does it follow that E and E' are isogenous over $\mathbf{Q}$?). We obtain a natural map

$$\psi_l : \mathrm{Hom}_M(A,B) \to \mathrm{Hom}(T_l A, T_l B).$$

(l some prime number, $l \neq \mathrm{char}\, M$). In general there is little chance that this map is bijective: the left-hand side is a free $\mathbf{Z}$-module of rank at most $4gg'$ ($g = \dim A$, $g' = \dim A'$; at most $2gg'$ if $\mathrm{char}(M)=0$), and the right-hand side is isomorphic (as a group) to $(\mathbf{Z}_l)^{4gg'}$; of course $- \otimes_{\mathbf{Z}} \mathbf{Z}_l$ to the left-hand side will help, but still there is no chance in general that the map is bijective. The Tate conjecture reads (cf. [Ta1], page 134, last paragraph):

(T). *Let M be a field which is finitely generated over its prime field. Then for every A and B (abelian varieties over M) and for every $l \neq \mathrm{char}(M)$ the map*

$$\psi_l : \mathrm{Hom}_M(A,B) \otimes \mathbf{Z}_l \to (\mathrm{Hom}(T_l A, T_l B))^G$$

is bijective and

$$\mathrm{End}((T_l A \otimes \mathbf{Q}_l) \textit{ is a semi-simple } G\textit{-module}$$

(here $G:=\mathrm{Gal}(M^s/M)$ and the superscript G indicates that only those homomorphisms which commute with the action of G should be taken, and finally $\mathbb{Q}_l$ = field of fractions of $\mathbb{Z}_l$).

In [Ta1] TATE proved this in the case the $M=\mathbb{F}_q$ is a finite field. FALTINGS proved (T) in the case $M=K$, a number field. This has important consequences, e.g., let A and B be abelian varieties over a number field have the same zeta function, then they are isogenous. Thus one asserts the existence of a morphism from apparently weaker data! See ZARHIN [Za4] and MORET-BAILLEY [MB] for other cases of the Tate conjecture; also cf. [FW]. I think this theorem will have many applications in the future.

As already remarked, we are not going to enter in the proof of (Sh) and of (T) (and hence of (M)). Let me only note that FALTINGS first proves weak forms of (Sh), then using such finiteness results one derives (T) as indicated on page 137 of [Ta1] and given by ZARHIN in [Za4]; then a beautiful (and short!) argument using deep facts like the Chebotarev density theorem and Weil's Riemann hypothesis for abelian varieties finishes the proof of (Sh). The proof is both elegant and quite involved, the results are astonishing.

8. THE FUNCTION FIELD CASE

Let k be a field, let B be an affine curve over k with coordinate ring R (and suppose B is smooth). In this case we speak of the function field case, $M=k(B)$ is a function field in one variable. There are striking analogies between the function field case and the arithmetic case. That analogy seems very stimulating. Already many mathematicians studied it fruitfully, and we would need quite a lot of space to give an adequate description. Note that R is a Dedekind domain, just as in the case of the ring of integers in a number field. E.g. by using of the theory of minimal models, a curve C over $k(B)$ can be extended to a surface $\mathcal{C}$ with a morphism $\mathcal{C}\rightarrow B$ having C over $k(B)$ as generic fibre. Thus we see that methods of surfaces hopefully can be transported to the arithmetic case etc.

From the rich variety of problems and results we like to mention only two.

If we want to settle a certain problem in arithmetical algebraic geometry, it sometimes helps to decide first the case of a function field as a starting point. E.g. the Mordell conjecture was proved for function fields by MANIN (in characteristic zero, cf. [Ma1]), and by GRAUERT (in the algebraic case, cf. [Gr]). One has to make certain restrictions, e.g. if C is a curve over a field k with $\#C(k)$ not finite, then for any $M\supset k$ the 'constant' curve $C\otimes_k M$ certainly has infinitely many M-rational points. But these restrictions are quite natural. The 'Shafarevich-Mordell conjecture in the function field case' has obtained much attention. We mention only results by PARSHIN, cf. [Pa1], ARAKELOV, cf. [Ar1], SZPIRO, cf. [Sz] (and there are many more). Here, results on algebraic surfaces are useful: take $\mathcal{C}\rightarrow B$, a fibering by curves over a curve B, compactify B, extend $\mathcal{C}$ to a complete surface, and try to compute all kinds of invariants of this surface (cf. [Ar1], pp. 1298-1301). But also deformation theory ('rigidity theorems') comes in: one proves that the objects in consideration are rigid and belong to bounded families (and finiteness follows). This line of thought is exposed in [Mu], pp. 41-43. Certainly this field of research will produce more interesting theorems.

As said, often the function field case is used as a test case for the arithmetic case. If one wants to prove a theorem for curves or for abelian varieties over number fields, one can first analyze the analogous situation in the function field case (either with k a finite field, or with $k=\mathbb{C}$, imposing extra restrictions). Thus it was surprising to see that the Shafarevich philosophy is correct for abelian varieties over number fields, whereas FALTINGS in [Fa1] shows that the analogous finiteness theorem for families of principally polarized abelian varieties with zero trace (i.e. non-constant in a very strong form) does not hold for abelian varieties of dimension eight (!) in case of function fields of characteristic zero (possibly there is a relation with new results by SERRE on l-adic representations). Thus here the arithmetic case has no exceptions (which makes life easy, e.g. replace A by $A^4 \times (A^t)^4$), whereas in the function field case one has to be more careful.

We mentioned already the following method: if $\mathcal{C} \rightarrow B$ is a fibering of curves over a curve, compactify B to a complete curve, replace $\mathcal{C}$ by a complete surface

$$\overline{\mathcal{C}} \rightarrow \overline{B}$$

and apply the theory of compact surfaces. This method, which is rather obvious in the function field case, can be imitated in the arithmetic case. If C is a curve over a number field K, let R be the ring of integers of K, and $B:=\mathrm{Spec}(R)$, with $\mathcal{C} \rightarrow B$ an extension of C to B (e.g. via minimal models). ARAKELOV and FALTINGS have developed a theory of 'arithmetic surfaces' ($\mathcal{C}$ has Krull-dimension equal to two) which also takes into account intersections at infinity, cf. [Ar2], [Fa2]. Certainly this abuts to ideas which go back to WEIL and KRONECKER (cf. Weil's talks [1939a] 'Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques' and [1950b] 'Number theory and algebraic geometry' in [We4], Vol. I and Vol. II). Several basic facts about number fields and theorems on algebraic curves are merely translations of each other. In this way we obtain a geometric interpretation (and intuition) for certain algebraic concepts (an explanation of the height as a degree of a certain line bundle is an example cf. [F], p.354; these concepts play an essential role in the proof of (Sh), (T) and (M)). Geometry leads us to the correct concepts in this part of number theory. It seems that 'arithmetical algebraic geometry' is in a rapid of developments.

9. A FINAL REMARK

After having mentioned these beautiful and influential results I would like to make a remark on the style in which they are written down in the paper [F].

For centuries mathematicians have struggled with deciding on the precision in which mathematical achievements are to be recorded. Many concise mathematical papers are only understandable for a small circle of insiders. But often we see that when an author tries to make every argument precise, tries to capture every property in a symbol, the result can be an indigestible paper or book. So we like to make descriptions and notation transparent so as to unveil the true ideas and deep motivations for the theory. There is a variety in styles, ranging from extensive treatises to concise descriptions of the essentials. As to Falting's paper I would like to make the following remarks in this respect.

At several places the author just says enough to give the basic ideas without burying it under heaps of notation; to my taste this reflects the deep insight the author has in these intricate matters, and it is stimulating to try to follow the surprising way leading to these results. However, I feel, at some places the author is too brief in this paper. At some places the author gives hints only understandable for the experts, at several places references are lacking (e.g. on p.365: 'Beweis Torelli'; it would be easy to give a reference, and then some details still have to be filled in, because Torelli's theorem is formulated over an algebraically closed field; a combination of these two little obstacles makes the paper difficult for non-specialists at such a point); I feel the author could have given more references. Furthermore, I have one fundamental criticism; the author uses ambiguous notation, and he uses references in a way that does not quite fit his situation. Thus even for specialists it becomes a difficult affair to check details of this proof. It could have been avoided with more precision. With such a style mistakes can be made more easily. It seems dangerous if such a style would become daily practice in mathematics. I must give an example to illustrate my critical remark. On p.364 of [F] we find on line 11 an isogeny between abelian varieties, and its kernel is denoted by G. We have seen in the paper that the author uses the same kind of symbols for an abelian variety over a field (A over K), and for an extension ('let $A \rightarrow S$ be a semi-abelian variety'; here R is the ring of integers of K, and $S = \mathrm{Spec}(R)$; many authors distinguish $\mathcal{A} \rightarrow S$ and $\mathcal{A} \otimes_R K = A$, but FALTINGS uses the same notation in both cases). The use of the words 'abelian varieties' leads to the conclusion that we work over a field, so $G = \mathrm{Ker}\,\phi$ would then be a finite group scheme over K; but on line 7 from below we find $G \,/\, R$, so apparently G is considered as a group scheme over S; the most logical guess gives a group scheme $G \rightarrow S$ which is quasi-finite over S, but in general not finite over S! At the places where the abelian varieties have bad reduction, the group scheme may fail to be finite. At that moment FALTINGS refers to a result by RAYNAUD, but that result is valid for finite group schemes. The reference serves to compute a certain ramification, but if one wants to complete the quasi-finite group scheme to a finite one, this may create 'new ramification'. This is not something which can be settled by a simple and direct argument, although the case considered can be settled (cf. [D], p.13 and p.15), and finally the result seems correct (except for [F], Satz 2 in that form). Personally I feel a style is not acceptable if it is difficult even for insiders to check details of the proof.

Certainly this small point will not diminish my enthusiasm and respect for these results. Coming generations may judge whether this is 'the theorem of the century'. In the meantime, we can gratefully enjoy and use the new developments.

REFERENCES

F G. FALTINGS. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math. 73 (1983)*, 349-366 (Erratum, *Invent. Math. 75 (1984)*, 381).

D P. DELIGNE. Preuve des conjectures de Tate et de Shafarevich [d'après G. Faltings]. *Sém. Bourbaki 36 (1983/1984)*, No. 616.

S L. SZPIRO. La conjecture de Mordell [d'après G. Faltings]. *Sém. Bourbaki 36 (1983/1984)*, No. 619.

An A. ANDREOTTI. On a theorem of Torelli. *Amer. J. Math. 80 (1958)*, 801-828.

AAG *Arithmetical Algebraic Geometry*. O.F.G. SCHILLING (ed.). *Proceed. Conf. Purdue Univ. 1963*, Harper & Row, 1963.

Ab V.A. ABRASHKIN. p-divisible groups over $\mathbb{Z}$. *Izv. Akad. Nauk SSSR Ser. Mat. Tom 41 (1977)* [*Math. USSR Izvestija 11 (1977)*, 937-956].

ANT *Algebraic Number Theory*. J.W.S. CASSELS, A. FROLICH (eds). *Proceed. Conf. Brighton 1965*, Academic Press, 1967.

Ar1 S.JU. ARAKELOV. Families of algebraic curves with fixed degeneracies. *Izv. Akad. Nauk SSSR 35 (1971)* [*Math. USSR Izvestija 5 (1971)*, 1277-1302].

Ar2 S.JU ARAKELOV. Intersection theory of divisors on an arithmetic surface. *Izv. Akad. Nauk SSSR 38 (1974)* [*Math. USSR Izvestija 8 (1974)*, 1167-1180].

Ch S. CHOWLA. Proof of a conjecture of Julia Robinson. *Kong. Norske Vid. Selsk. Forh. (Trondheim) 34 (1961)*, 100-101.

Fa1 G. FALTINGS. Arakelov's theorem for abelian varieties. *Invent. Math. 73 (1983)*, 337-347.

Fa2 G. FALTINGS. Calculus on arithmetic surfaces. *Ann. Math. 119 (1984)*, 387-424.

Fa3 G. FALTINGS. Die Vermuting von Tate und Mordell. *Jber. Dt. Math.-Verein 86 (1984)*, 1-13.

Gr H. GRAUERT. Mordells Vermuting über rationale Punkte auf algebraischen Kurven und Funktionenkörper. *Publ. Math. IHES, No. 25 (1965)*, 363-381.

HAG R. HARTSHORNE. *Algebraic Geometry. Grad. Texts Math. 52*, Springer-Verlag, 1977.

Ha H. HASSE. *Zahlentheorie*, Akad. Verlag, Berlin, 1963.

Ka A. KAS. On deformations of a certain type of irregular algebraic surface. *Amer. J. Math. 90 (1968)*, 789-804.

Ko K. KODAIRA. A certain type of irregular algebraic surfaces. *Journ. Analyse Math. 19 (1967)*, 207-215.

La1 S. LANG. *Abelian Varieties*, Intersc. Publ., 1959.

La2 S. LANG. Division points on curves. *Annali Mat. Pura Appl. Ser. IV, 70 (1965),* 229-234.

La3 S. LANG. *Fundamentals of Diophantine Geometry,* Springer-Verlag, 1983.

LMO J.C. LAGARIAS, H.L. MONTGOMMERY, A.M. ODLYZKO. A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math. 54 (1979),* 271-296.

Ma1 JU.I MANIN. A proof of the analog of the Mordell conjecture for algebraic curves over function fields. *Dokl. Akad. Nauk SSSR 152 (1963),* 1061-1063 [*Soviet Math. 4 (1963),* 1505-1507].

Ma2 JU.I. MANIN. Rational points of algebraic curves over function fields. *Izvestija Akad. Nauk 27 (1966),* 1395-1440 [*Amer. Math. Soc. Translat. Ser. 2, 50* (1966), 189-234].

Maz B. MAZUR. *Modular Curves and the Eisenstein Ideal. Publ. Math. No.47 (1977),* IHES.

Mo1 L.J. MORDELL. On the rational solutions of the indeterminate equations of the 3rd and 4th degrees. *Proc. Cambridge Phil. Soc. 21 (1922),* 179-192.

Mo2 L.J. MORDELL. *Diophantine Equations,* Academic Press, 1969.

M-B L. MORET-BAILLY. Variétés abéliennes polarisées sur les corps de fonctions. *C.R. Acad. Sci Paris 296 (1983),* 267-270.

GIT D. MUMFORD. *Geometric Invariant Theory. Ergebnisse, Vol. 34.* Springer-Verlag, 1965.

MAV D. MUMFORD. *Abelian Varieties. Tata Inst. Fund. Research, Stud. Math. Vol. 6* Tata Inst. F.R., Bombay, and Oxford Univ. Press, 1979.

Mu D. MUMFORD. *Curves and their Jacobians.* The Univ. Michigan Press, Ann Arbor, 1975.

Ogg A.P. OGG. Abelian curves of 2-power conductor. *Proc. Cambridge Phil. Soc. 62 (1966),* 143-148.

Oo1 F. OORT. *Commutative Group Schemes. Lecture Notes Math. 15,* Springer-Verlag, 1966.

Oo2 F. OORT. (1973). The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field. *Journ. Pure Appl. Algebra 3 (1973),* 339-408.

Oo3 F. OORT. Elliptic curves: diophantine torsion solutions and singular j-invariants. *Math. Ann. 207 (1974),* 139-162.

Oo4 F. OORT. Good and stable reduction of abelian varieties. *Manuscr. Math. 11 (1974),* 171-197.

Oo5 F. OORT. Subvarieties of moduli spaces. *Invent Math. 24 (1974),* 95-119.

Oo6 F. OORT. Hyperelliptic curves over number fields. H. POPP (ed.): *Classification of Algebraic Varieties and Compact Complex Manifolds. Lect. Notes Math. 412,* Springer-Verlag, 1974; 211-218.

OS F. OORT, J. STEENBRINK. The local Torelli problem for algebraic curves. A. BEAUVILLE (ed.): *Journ. Géom. Algébrique Angers 1979,* Sijthoff & Noordhoff, 1980; 157-204.

OU F. OORT, K. UENO. Principally polarized abelian varieties of dimension two or three are Jacobian varieties. *Journ. Fac. Sc., The Univ. Tokyo, Sec. IA, 20 (1973),* 377-381.

Pa1 A.N. PARSHIN. Algebraic curves over function fields, I. *Izv. Akad. Nauk SSSR 32 (1968),* 1191-1219 [*Math. USSR Izvestija 2 (1968),* 1145-1170].

Pa2 A.N. PARSHIN. Quelques conjectures de finitude en géométrie diophantienne. *Actes, Congrès Intern. Math. 1970, I,* 467-471, Gauthier-Villars, 1971.

Pa3 A.N. PARSHIN. Minimal models of curves of genus 2 and homomorphisms of abelian varieties defined over a field of finite characteristics. *Izv. Akad. Nauk SSSR 36 (1972)* [*Math. USSR Izvestija 6 (1972),* 65-108].

Proc. *Proceedings Sympos. Pure Math. Vol. 28 (Part 1, Part 2).* Math. developments arising from Hilbert problems. AMS; 1976.

Ra1 M. RAYNAUD. Modèles de Néron. *C.R. Acad. Sc. Paris* 262 (1966), A345-347.

Ra2 M. RAYNAUD. Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. Math. France 102 (1974),* 241-280.

Ra3 M. RAYNAUD. Courbes sur une variété abélienne et points de torsion. *Invent. Math. 71 (1983),* 207-233.

Sa P. SAMUEL. *Théorie algébrique des nombres,* Hermann, 1967.

SemSz Séminaire sur les pinceaux de courbes de genre au moins deux. L. SZPIRO (ed.). *Astérisque 86. Soc. Math. France,* 1981.

FAC J.-P. SERRE. Faisceaux algébriques cohérents. *Ann. Math. 61 (1955),* 197-278.

Ga J.-P. SERRE. *Groupes algébriques et corps de classes. Act. Sc. Ind. 1264,* Hermann, 1959.

CL J.-P. SERRE. *Corps locaux. Act. Sc. Ind. 1296,* Hermann, 1962.

Se4 J.-P. SERRE. *Cohomologie galoisienne. Lecture Notes Math. 5,* Springer-Verlag, 1964.

Se5 J.-P. SERRE. *Abelian l-adic Representations,* Benjamin, 1968.

Se6 J.-P. SERRE. Propriétés galoisiennes des points d'ordre fini des courbes algébriques. *Invent. Math. 15 (1972),* 259-331.

Se7 J.-P. SERRE. Quelques applications des théorèmes de densité de Chebotarev. *Publ. Math. No. 54. IHES (1981),* 123-202.

ST J.-P. SERRE, J. TATE. Good reduction of abelian varieties. *Ann. Math. 88 (1968),* 492-517.

Sh I.R. SHAFAREVICH. Algebraic number fields. *Proc. ICM. Stockholm 1962,* 163-176 [*Amer. Math. Soc. Translat. 31,* (1963), 25-39].

Sz L. SZPIRO. Sur le théorème de rigidité de Parsin et Arakelov. *Journ. Géom. Alg. Rennes, 1978, Vol. II: Astérisque 64, Soc. Math. France (1979);* 169-202.

Ta1 J. TATE. Endomorphisms of abelian varieties over finite fields. *Invent. Math. 2 (1966),* 134-144.

Ta2 J. TATE. p-divisible groups. *Proceed. Conference Local Fields (Driebergen 1966),* 158-183, Springer-Verlag, 1967.

TO J. TATE, F. OORT. Group schemes of prime order. *Ann. Sc. École Norm Sup 3 (1970),* 1-21.

WM W.C. WATERHOUSE, J.S. MILNE. Abelian varieties over finite fields. Proceed. Symp. Pure Math. Vol. 20: 1969 Number Theory Inst. (Stony Brook). *Amer. Math. Soc. (1971),* 53-63.

We1 A. WEIL. L'Arithmétique sur les courbes algébriques. *Acta Math. 52 (1928),* 281-315.

We2 A. WEIL. *Sur les courbes algébriques et les variétés qui s'en deduisent. Act. Sc. Ind. 1041,* Hermann, 1948.

We3 A. WEIL. *Variétés abéliennes et courbes algébriques. Act. Sc. Ind. 1064,* Hermann, 1948.

We4 A. WEIL. *Oeuvres scientifiques. Collected Papers. Vol. I (1926-1931), Vol. II (1951-1964), Vol. III (1964-1978),* Springer—Verlag, 1979.

We5 A. WEIL. Sur les origines de la géométrie algébrique. *Compos. Math. 44 (1981),* 395-406.

Za1 JU.G. ZARHIN. Isogenies of abelian varieties over fields of finite characteristics. *Mat. Sbornik 95 (137) (1974)* [*Math. USSR Sbornik 24 (1974),* 451-461].

Za2 JU.G. ZARHIN. A remark on endomorphisms of abelian varieties over function fields of finite characteristics. *Izv. Akad. Nauk SSSR 38 (1974)* [*Math. USSR Izvestija 8 (1974),* 477-480].

Za3 JU.G. ZARHIN. Finiteness theorem for isogenies of abelian varieties over function fields of finite characteristics. *Functional Analysis and Appl. 8 (1974),* 301-303.

Za4 JU.G. ZARHIN. Abelian varieties in characteristic p. *Math. Notes 19 (1976),* 240-244.

Maz2 B. MAZUR. On the arithmetic of curves. *Lect. Notes AMS Meeting January 1984,* Louisville, Kentucky. AMS Colloquium Lecture Series (a beautiful survey paper, certainly accessible to non-specialists with a wealth of interesting remarks and problems).

FW G. FALTINGS, G. WÜSTHOLZ ET AL. *Rational Points. Aspects of Math. Vol. E6,* Vieweg (1984) (these are notes of the Bonn/Wuppertal seminar, 1983/84; in this book we find many details and new results about the theory treated in the papers by Faltings cited [F] and [Fa 2] above).