CWI NEWSLETTER

Centrum voor Wiskunde en Informatica
Centre for Mathematics and Computer Science

Quarterly, Issue no. 5
December 1984

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

CWI NEWSLETTER

Number 5, December 1984

Editors

Arjeh M. Cohen Richard D. Gill Jan Heering

The CWI Newsletter is published quarterly by the Centre for Mathematics and Computer Science (Centrum voor Wiskunde en Informatica), Kruislaan 413, 1098 SJ Amsterdam, The Netherlands. The Newsletter will report on activities being conducted at the Centre and will also contain articles of general interest in the fields of Mathematics and Computer Science, including book reviews and mathematical entertainment. The editors encourage persons outside and in the Centre to contribute to the Newsletter. Normal referee procedures will apply to all articles submitted.

The Newsletter is available free of charge to all interested persons. The Newsletter is available to libraries on an exchange basis.

All correspondence should be addressed to: *The CWI Newsletter, Centre for Mathematics and Computer Science, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands.*

ISSN 0168-826x

The cover shows Fermat's 'last theorem' as it first appeared in print in Bachet's annotated edition of Diophantus' *Arithmetica* of 1670. According to Fermat the diophantine equation $x^n + y^n = z^n$ does not have solutions for $n > 2$. Whether this is true or not is still unknown, but it follows from the recent work of Faltings that there are at most a *finite* number of solutions for every $n > 2$. See Oort's article in this issue.

Contents

CWI

Centre for Mathematics and Computer Science

Centrum voor Wiskunde en Informatica

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 $t \in \mathbb{Q}$,

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

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 $x,y \in \mathbb{Q}$. For cubic equations the situation is already much more complicated. Consider:

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

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

$$X^3+Y^3 = 1 \tag{4};$$

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 $\mathbb{Q}$, 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 $C(\mathbb{C})$. If C is a curve in the projective plane $\mathbb{P}^2$, 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:

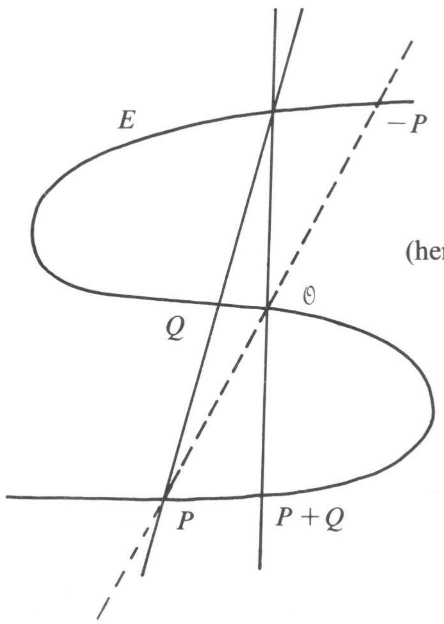
$x,y \in \mathbb{Q}$ or $x,y \in \mathbb{Z}$, with $f(x,y) = 0$.

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 $C(\mathbb{Q})\neq\emptyset$ 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, $E\subset\mathbb{P}^2$, 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 $E(\mathbb{Q})$ is *finitely generated*

(cf. [Mo1]); hence

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

with $r\in\mathbb{Z}_{\geqslant 0}$ and T a finite commutative group, $T=\mathrm{Tors}(E(\mathbb{Q}))$, the torsion subgroup of $E(\mathbb{Q})$. This theorem can be generalized, as A. WEIL proved: for any abelian variety A over a number field K (i.e. $[K:\mathbb{Q}]<\infty$), 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 $T=\mathrm{Tors}(E(\mathbb{Q}))$, 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 $\mathbb{Q}$), let C be an algebraic curve over K, assume $g(C)\geqslant 2$, then $\#(C(K))<\infty$.*

Note, as a corollary:

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

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 $\mathbb{Q}$ (by $4X=\xi$, $8Y=\eta$), they are not isomorphic over $\mathbb{Z}$, the point ($\xi=1$, $\eta=-5$) is an integral solution of the second equation but the corresponding $\mathbb{Q}$-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 $\mathbb{Q}$'.

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 $K=\mathbb{Q}$, $S=\varnothing$, $R=\mathbb{Z}$, 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 $a\in\mathbb{Z}$, $b\in\mathbb{Z}$ 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, $\overline{C}$ the compactification of $\mathcal{C}\otimes_R K$. Then $\mathcal{C}(R)$ is finite in each of the following cases:

(0) $g=0$, $\#(\overline{C}(\overline{K})-C(\overline{K}))\geqslant 3$;
(1) $g=1$, $\#(\overline{C}(\overline{K})-C(\overline{K}))\geqslant 1$;
($\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 $n \in \mathbb{Z}_{\geqslant 1}$ 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

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

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, $g \geqslant 1$, 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 $g \in \mathbb{Z}_{\geqslant 1}$; 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) $\Rightarrow$ (M), AND (Sh) $\Rightarrow$ (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 $\mathcal{C} \rightarrow Spec(R)$ (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 $C_1 \rightarrow C$ by pulling back $q \cdot id_J$ (where $J = \mathrm{Jac}(C)$);

$$\begin{array}{ccccc} & C_1 & \rightarrow & J & \\ f & \downarrow & & \downarrow & q \\ & C & \rightarrow & J, & \end{array}$$

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

$$C_P \rightarrow C'$$

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 $C' \rightarrow C$ and $C_P \rightarrow C'$). 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

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

this bounds the degree of K_P' and K_P' / K is unramified for all discrete valuations v with $v \mid 2$ 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 $w \mid v$ 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 $C_P \rightarrow C' \rightarrow C$ to $\mathrm{Spec}(R_w)$). Thus we arrive at a map:

$$P \mapsto C_P$$

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

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 $C_P \rightarrow C$ 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 $\mathbb{Q}$, the geometric method has to work via a large extension of $\mathbb{Q}$, 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 $x, y, z \in \mathbb{Z}$ 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 Jac(C). Thus one is naturally led to the study of abelian varieties. We denote for any $n \in \mathbb{Z}_{\geqslant 1}$ 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 char(M) does not divide n, then

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

(this is easy if char(M)=0, once you know that

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

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

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

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

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

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 $\mathbb{Q}$, 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 $\mathbb{Q}$?). 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 $\mathbb{Z}$-module of rank at most $4gg'$ ($g = \dim A$, $g' = \dim A'$; at most $2gg'$ if char(M)=0), and the right-hand side is isomorphic (as a group) to $(\mathbb{Z}_l)^{4gg'}$; of course $- \otimes_{\mathbb{Z}} \mathbb{Z}_l$ 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 $l \neq$ char(M) the map*

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

is bijective and

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

(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 $\mathcal{C} \to B$ is a fibering of curves over a curve, compactify B to a complete curve, replace $\mathcal{C}$ by a complete surface

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

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 $\mathcal{C} \to B$ 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 $A \to S$ be a semi-abelian variety'; here R is the ring of integers of K, and $S = \mathrm{Spec}(R)$; many authors distinguish $\mathcal{A} \to S$ 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 $G \to S$ 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).

Proportional representation in a regional council

J.M. Anthonisse
Centre for Mathematics and Computer Science
Kruislaan 413
1098 SJ Amsterdam
The Netherlands

The members of a regional council are appointed by and from the local councils which participate in the regional cooperation.
The regional council should constitute a fair representation of the local interests and also a fair representation of the political views.
A method is presented to determine the number of members to be appointed by each local council from each political party. Optimal flows in networks solve the problem.

1. Introduction

The region *Gooi en Vechtstreek* is a cooperation of nine municipalities near Amsterdam. The statute of the cooperation stipulates that the members of the regional council are appointed by the participating local councils. Each local council has an odd number of members, a fourth part of which (rounded to the nearest integer) is appointed into the regional council. In this way, the representation of each municipality is proportional to the membership of its council and this should be a fair representation of the local interests in the regional cooperation.

The regional council should also be a fair representation of the political views on the matters to be discussed and decided by that body. Each political party should get a number of seats in the regional council that is close to a fourth part of its total number of seats in the local councils. Thus, if a party has a single seat in each local council then it expects to get two seats in the regional council. However, if the allocation of seats is completely left to the local councils then it may be expected that none of these will give a seat in the regional council to a small minority in their midst, if only for fear that the other councils would do so too. It is clear that the local councils should coordinate the allocation of seats so as to obtain a fair political composition of the regional council.

In *Gooi en Vechtstreek* the allocation of seats is coordinated by the chairman of the cooperation. Based on the outcome of the local elections he calculates the number of seats to be allotted to each party in each local council. The results of his calculations are discussed with the incumbent political leaders of the regional council and then sent, as an advice, to the local councils. In 1982 the method as described by Anthonisse [1] was used. The present paper provides an extended and improved method.

In the Netherlands, cooperation between municipalities is quite common. There are 740 municipalities and over 1250 cooperations. Many cooperations have a very restricted purpose and the political composition of their council is not important. A new law, to become effective 1st January 1985, should improve the surveyability of the cooperations. The country is to be divided into regions of cooperation and, as a rule, cooperation will be restricted to the municipalities in a region. Moreover, the number of cooperations will be reduced by integrating several existing cooperations into a new one. The new law stipulates that the councils are appointed by and from the local councils. The statute of the cooperation must specify the number of members to be appointed by each local council.

It may be expected that, due to these developments, there will be an increased interest in the political composition of the councils of cooperations.

2. Proportional representation as an optimization problem

The problem of proportional representation is to allot the seats in a representative body to the political parties in such a way that the number of seats is proportional to the number of votes for each party. Let v_p denote the number of votes for party p, thus the total number of votes is $V = \sum_p v_p$. Let S denote the number of seats in the body, then party p should obtain $e_p = S \times v_p / V$ seats. In general, however, the numbers e_p are not integers and rounding is required to obtain a feasible allotment. Let s_p denote the number of seats for party p.

Te Riele [2] describes seven methods of proportional representation as methods to solve an optimization problem

$$\text{minimize} \sum_p f(e_p, s_p) \tag{1}$$

subject to

$$\sum_p s_p = S \tag{2}$$

and

$$\text{each } s_p \text{ non-negative integer.} \tag{3}$$

The function $f(e_p, s_p)$ determines the distance between the exact or theoretical allotment e_p and the solution s_p.

The well-known method of the greatest remainders (Roget, Hamilton) corresponds with

$$f(e_p, s_p) = |e_p - s_p|. \tag{4}$$

The equally well-known method of the greatest divisors (D'Hondt, Hagenbach-Bischoff, Jefferson) corresponds with

$$f(e_p, s_p) = (s_p - (e_p - \tfrac{1}{2}))^2 / e_p. \tag{5}$$

Webster's method corresponds with

$$f(e_p,s_p) = (s_p - e_p)^2 / e_p. \quad (6)$$

BALINSKI and YOUNG [3] list a number of properties of the 'ideal' method of proportional representation and show that no such method exists.

The method of the greatest remainders allows the occurrence of the Alabama-paradox: while the v_p remain the same, an s_p may decrease by increasing S. A fair method should not allow this.

The method of the greatest divisors favours the greater parties. This method has a tendency to round e_p downwards as s_p is compared with $e_p - \frac{1}{2}$. However, some e_p must be rounded upwards and this will occur, in general, at the largest e_p.

WEBSTER's method appears to be a very good approximation to the ideal of proportional representation.

3. THE METHOD

Now the problem of allotting the seats in the regional council to the parties in the local councils can be formulated. Throughout $f(\cdot,\cdot)$ denotes any function corresponding with a method of proportional representation. The number of members of party p in the local council of municipality m is denoted by c_{mp}. Here a practical problem occurs, as it is not evident which parties should be distinguished. The municipal elections allot the seats in the local council to, typically, four up to six local parties. Some of these local parties are chapters of national parties, others are coalitions of such chapters and still others are purely local political organizations. Thus it must be decided which combinations of local parties should be considered as regional parties in order to allot the seats in the regional council. A conclusive arrangement is to combine those local parties which, by a joint statement, require to be combined and to consider each remaining local party as a separate one. From these statements the c_{mp} can be determined. The regional strength of a party is $r_p = \sum_m c_{mp}$ and $R = \sum_p r_p$. The local council of m has $s_m = \sum_p c_{mp}$ seats.

Let a_m denote the number of members of the regional council to be appointed by and from the local council of municipality m. Thus $A = \sum_m a_m$ is the number of seats in the regional council. The numbers a_m are found by consulting the statute of the cooperation.

Now the allotment can be found by solving two problems. First, the political composition of the regional council is found by computing the number of seats b_p for each party p. Secondly, the numbers x_{mp} are computed, which denote the number of members of party p to be appointed from the local council of municipality m.

The first problem is to find b_p:

$$\text{minimize} \sum_p f(e_p,b_p) \quad (7)$$

subject to

$$\sum_p x_{mp} = a_m \quad (m = 1,2,...) \quad (8)$$

$$\sum_m x_{mp} = b_p \quad (p = 1,2,...) \tag{9}$$

$$x_{mp} \leqslant c_{mp} \quad (m = 1,2,...;\ p = 1,2,...) \tag{10}$$

and

$$\text{each } b_p, x_{mp} \text{ non-negative integer,} \tag{11}$$

where e_p denotes a theoretical allotment of the A seats, e.g. $e_p = A \times r_p / R$.

The second problem is to find x_{mp}:

$$\text{minimize} \sum_m \sum_p f(e_{mp}, x_{mp}) \tag{12}$$

subject to

$$\sum_p x_{mp} = a_m \quad (m = 1,2,...) \tag{13}$$

$$\sum_m x_{mp} = b_p \quad (p = 1,2,...) \tag{14}$$

$$x_{mp} \leqslant c_{mp} \quad (m = 1,2,...;\ p = 1,2,...) \tag{15}$$

and

$$\text{each } x_{mp} \text{ non-negative integer,} \tag{16}$$

where b_p denotes the solution of the first problem and e_{mp} denotes a theoretical allotment of the seats, e.g. $e_{mp} = A \times c_{mp} / R$.

The first problem obviously has a feasible solution, provided $a_m \leqslant s_m$. The latter condition is certainly satisfied, thus any sample of a_m from the s_m members satisfies (8) and (10). Constraint (9) merely defines b_p.

It is clear that the second problem, with the b_p which solve the first one, also has a feasible solution. Constraints (8)-(11) are identical to constraints (13)-(16).

It is tempting to replace the first problem by a simpler one. The b_p might be computed by allotting the A seats proportional to r_p. This amounts to a relaxation of the constraints (8)-(11) into

$$\sum_p b_p = A$$
$$b_p \text{ non-negative integer.} \tag{17}$$

However, this may yield a nonfeasible second problem, as the following example shows.

c_{mp}	$p=$ 1	2	3	4	5	6	a_m	
$m=1$	7						2	
2	7						2	
3	7						2	
4	6	1					2	
5		30	15				11	
6			16	29			11	
7				2	31	12	11	
8						19	5	
b_p	6	8	8	8	8	8	46	$=A$

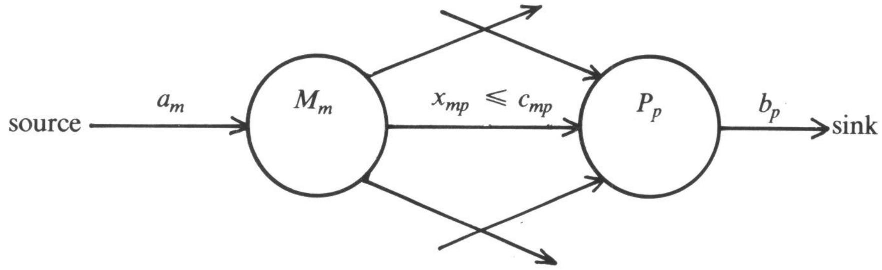
The method of the greatest remainders was used here to determine the b_p proportional to (27,31,31,31,31,31). This results in 6 seats for party 1, but this party will get at least 7 seats from the first four municipalities. Similar examples have been constructed for other methods of proportional representation.

Thus the first problem must be solved to ensure the feasibility of the second problem.

In practice, however, the simpler method (7), (17) to compute b_p may be tried first. If, with these b_p, the second problem is feasible then these b_p constitute an optimal solution of the first problem. In the opposite case the problem (7)-(11) must be solved to obtain the correct b_p.

4. Flows in networks

Both the first and the second problem as defined in the previous section can be formulated as problems of finding an optimal flow in a network. In both cases the network contains nodes M_m corresponding with the municipalities and P_p corresponding with the parties. Node M_m receives a fixed flow of a_m units from a source. The arc from M_m to P_p has a capacity of c_{mp} units, the flow in this arc is denoted by x_{mp}. There is a flow of b_p units from node P_p into a sink. At each node, the incoming flow equals the outgoing flow.



In the first problem, $f(e_p, b_p)$ can be interpreted as the cost of sending b_p units of flow from node P_p towards the sink. The problem is to find a feasible flow which minimizes these costs. Most algorithms to solve such problems assume that the cost is a linear function of the flow through an arc. Due to the convexity of $f(e_p, b_p)$ the problem is easily put into this form.

Let $\hat{b}_p$ denote an integer value of b_p which minimizes $f(e_p, b_p)$. Then

$$b_p = \hat{b}_p + (b_{p1}^+ + b_{p2}^+ + \cdots) - (b_{p1}^- + b_{p2}^- + \cdots)$$

where

$$b_{pi}^+ \in \{0,1\} \quad \text{and} \quad b_{pi}^- \in \{0,1\}.$$

Then

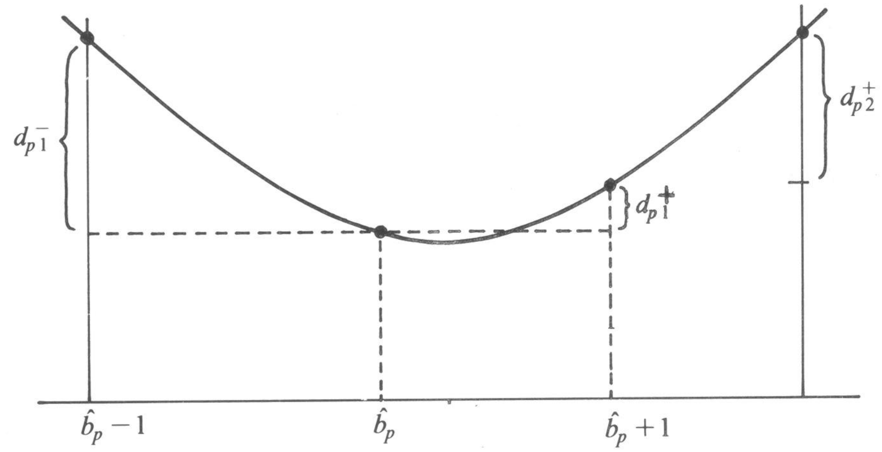
$$f(e_p, b_p) = f(e_p, \hat{b}_p) + \sum_i d_{pi}^+ b_{pi}^+ + \sum_i d_{pi}^- b_{pi}^-$$

where

$$d_{pi}^+ = f(e_p, \hat{b}_p + i) - f(e_p, \hat{b}_p + i - 1)$$

and

$$d_{pi}^- = f(e_p, \hat{b}_p - i) - f(e_p, \hat{b}_p - i + 1).$$



Now the arc from P_p towards the sink having a nonlinear cost can be replaced by a number of parallel arcs. One contains a fixed flow of $\hat{b}_p$ units. The other arcs have unit capacity. Some of the arcs are directed from P_p towards the sink. These correspond with flows b_{pi}^+ at cost d_{pi}^+. Other arcs are directed from the sink towards P_p. These correspond with flows b_{pi}^+ at cost d_{pi}^-. The mincost flow in this network corresponds with the solution of the first problem.

In the second problem, the flows from P_p towards the sink are fixed at b_p. Now the mincost flow between the nodes M_m and P_p is to be found. Again, the problem can be linearized by replacing the arcs from M_m to P_p by parallel arcs in both directions, with the appropriate capacities and costs.

With the above linearizations the two problems are easily solved, either by a network flow algorithm or by a general algorithm for linear programming. The first complete treatment of flows in networks was given by FORD and FULKERSON [4]. The book by KENNINGTON and HELGASON [5] contains computer programs of flow algorithms. These programs are available in OPERAL, the CWI library of Operations Research Algorithms.

5. CONCLUDING REMARKS

The two problems defined above can be solved simultaneously as

$$\text{minimize } W_1 \sum_p f(e_p, b_p) + \sum_m \sum_p f(e_{mp}, x_{mp})$$

subject to (8)-(11), where W_1 denotes a sufficiently large value. For $W_1 = 0$ the optimal x_{mp} are completely defined by the local preferences and can be found by solving a proportional representation problem for each m separately. An increase of W_1 means that more weight is attached to the regional preferences.

It might occur that the statute specifies A only and that the a_m are to be found by solving a proportional representation problem. Now the three problems may be solved simultaneously

$$\text{minimize } W_0 \sum_m f(A \times s_M / R, a_m) + W_1 \sum_p f(e_p, b_p) + \sum_m \sum_p f(e_{mp}, x_{mp})$$

subject to (8)-(11) and

$$a_m \text{ non-negative integer and } \sum_m a_m = A,$$

where both W_0 and W_1 are sufficiently large.

As mentioned above, there is a wide choice of functions $f(\cdot,\cdot)$ that could be used in the above method.

Moreover, another definition of e_{mp} could be used, e.g. $e_{mp} = a_m \times c_{mp} / s_m$. These e_{mp} reflect the local preferences. By using these e_{mp} the composition of the regional council would not deviate more from the sum of the local preferences than is necessary to reflect the regional strength of the parties.

Also, another definition of e_p could be used, e.g., $e_p = \sum_m a_m \times c_{mp} / s_m$. This, however, introduces a bias because the a_m are not an exact proportional distribution of the A seats over the municipalities.

In the above description, the apportionment is based on the number of representatives in the local councils. They could also be based on the number of votes for a party.

Similar optimization models to the ones described above can be formulated to solve the other problems which may arise when the new law becomes effective.

REFERENCES

1. J.M. ANTHONISSE (1981). *Geografische en Politieke Samenstelling van de Gewestraad*, Gewest Gooi en Vechtstreek.
2. H.J.J. TE RIELE (1978). The proportional representation problem in the Second Chamber: an approach via minimal distances. *Statistica Neerlandica 32,* 163-179.
3. M.L. BALINSKI, H.P. YOUNG (1982). *Fair Representation,* Yale University Press, New Haven and London.
4. L.R. FORD, D.R. FULKERSON (1962). *Flows in Networks,* Princeton University Press, Princeton.
5. J.L. KENNINGTON, R.V. HELGASON (1980). *Algorithms for Network Programming,* Wiley, New York.

Living in Amsterdam

Steven Pemberton
Centre for Mathematics and Computer Science
Kruislaan 413
1098 SJ Amsterdam
The Netherlands

Having visited Holland before, I knew that they were going to ask me three questions at the border: 'How long are you staying? Have you got a return ticket? How much money have you got with you?' Since I guessed that at least two of my answers were going to be unsatisfactory to them, and so that I wouldn't be kept too long, I had my invitation letter from the Mathematical Centre (as the CWI was then called) close at hand, as I dragged my trunk the size of a small house along.

A friend had come with me to help me move in, and she went through passport-control first. How long was she staying? One week. Had she a return ticket? Yes. How much money did she have? 200 guilders. All satisfactory answers, and she got waved on. Then me. 'Are you together?' Yes, I said. 'Ok, you can go.' And that was it! I wonder what he thought I had in my trunk for a week's stay!

Amsterdam. City of canals, trams, bars that stay open later than 11 o'clock at night, and in Summer a hippy on every corner singing yet *more* Bob Dylan songs.

I was determined not to be the sort of Englishman abroad who only sticks with other English people, and whose house is a pocket of Englishness. No, I was going to merge in. I was going to be a real Amsterdammer.

Delight of Transport

One of the distinguishing features of Amsterdam is its wide range of transport facilities. More than half the working population of Amsterdam go to work under their own steam (in other words by foot or bike — while there's a lot of water, I still haven't heard of anybody who swims to work). And the canals with their opening bridges are a real way of life for Amsterdammers — it is said that half the people who are late for work use the excuse 'I'm sorry, the bridge was up'. The other half use the excuse that it was down.

On trams, what distinguishes tourists from Amsterdammers is that tourists don't pay, because they get on the tram with everyone else and then sit staring around wondering how you pay and whether a conductor is going to come and collect fares. Amsterdammers on the other hand just don't pay. They know how much the fine is, and how often you get one, and they know which is cheaper.

But of course the *real* Amsterdammer rides a bike, and so the first step for any aspiring Amsterdammer is to go to the Waterlooplein flea market and buy one. So that I duly did, a lovely job with three speeds. A week later I discovered the second step to becoming an Amsterdammer — you get it stolen.

In fact since then I've discovered a little known fact that may interest you. Cyclists must pay a cycle tax, and this is levied by taking your bike, and re-selling it (on the Waterlooplein flea market). The current tax rate is one bike per year: everyone that I asked how long they had lived here and how many bikes they had lost, always said the same number for both. Well, with one exception. A friend here at the CWI boasted to me that he hadn't had a bike stolen in four years. Alas, someone must have been listening, because by the end of that year he had had four stolen. (This story got around the CWI recently, and some more people started coming to me boasting. Foolish people who didn't recognise the warning in the last sentence. I especially pity the person who told me he'd had the same bike for 35 years...)

As an Englishman, people ask me 'Don't you find it difficult riding on the right?' but the answer is no. I believe that the world is divided into two sorts of people — those who read maps by turning the map round in the direction they're travelling, and those who do it by turning their brains round in the direction they're travelling. Being of the latter type, I just had to flip my brain over, and there were no problems. Well — except now with reading maps ...

No, it wasn't with left and right I had problems, but with colours. I still haven't got used to red traffic lights meaning 'go' for cyclists. And another thing. Having been a cyclist in a particularly hilly part of England, I was looking forward to coming to flat Amsterdam. What I hadn't anticipated was the compulsory passenger that you must carry on the back of your bike here. Terrible.

Street life

Another step to becoming a true Amsterdammer is to see a riot, and I think the police realised this, and so as a sort of welcoming gesture, organised a riot in my neighbourhood. I lived in a quiet street then, full of trees and birds, not your usual sort of street for a riot thus, and so one evening just as I was cycling home from work (on my second bike), the police chased some rioters into my street as a sort of 'surprise party', and proceeded to set about me with clubs.

Only that week I had learnt my first three Dutch sentences, and this was my big chance to try two of them out. After having received the legal minimum number of blows to my body, I was able to get up off the ground and blurt out 'Ik ben Engels. Ik woon in deze straat.' This seemed to convince him, despite, or perhaps because of, my bad Dutch, and he rudely pushed me out of the street with his stick, with some of his chums joining in for the fun.


LANGER DAN
UUR

That evening also gave me the chance to experience the wonderful new Academic Hospital on the outskirts of Amsterdam, having my arm X-rayed.

Two lips in Amsterdam

Learning Dutch is of course an important step to becoming a true Amsterdammer, and so as soon as I arrived in Holland, much to the surprise of many of my Dutch friends, I set about learning it. 'But it's such an unimportant language!' they would plead. But to tell the truth, I had always wanted to learn Dutch. I knew that after Frisian it is the closest living language to English (excluding American of course), and the idea of this fascinated me — I really wanted to see in what ways the two languages had diverged from their common source of a thousand odd years ago.

However, when I was in England I could find little justification for putting the effort into learning it. 'It's such an unimportant language' I would say to myself. And so coming to Amsterdam was my big opportunity.

It's not difficult to find the similarities between the two languages. One's first few weeks in Holland are filled with being charmed by sentences that are recognisably the same as English. 'Beter dan de rest!' proclaimed a bag of apples I bought at the greengrocers; on all the windows in trams, in jolly red letters, is the sign 'Wilt U zitten? Ik kan staan!', presumably some sort of subliminal suggestion to make you give up your seat as the tram fills, though the only time I tried it, I was greeted with gales of laughter.

Learning a language is a funny affair. For a start, the first thing you learn to say is 'I'm sorry I don't speak your language'. And another thing is, you can never ask a native speaker any but the simplest questions. I have a particular memory of one time I was complaining to a Dutchman about one especially difficult property of the language that I continually have problems with, and giving a few examples of how you had to say different things in very similar situations. He blinked at me blankly for a few moments, and then said 'Yes — why is that actually?'

The closeness of the two languages makes it relatively easy to learn for the English speaker, though of course relying on similarities can be very misleading. The word 'warm' for instance, looks identical in the two languages, but in Dutch I've found that it clearly means something much warmer than in English. I mean, who would be tempted by the offer of a 'warm meal'? Not I. And consider the words 'slim' and 'stout' that occur in both languages. Who would guess that in Dutch they mean respectively 'clever' and 'naughty'? (apart from the Dutch of course).

Interestingly enough, the two strongest words in the English language, the only two I believe that don't appear in the original edition of the Oxford English Dictionary (they added them in supplement I'm told), these two words have acceptable, everyday, but it must be admitted related, meanings in Dutch. It is initially quite a shock to hear them being used in polite company, the sort of shock an English person experiences when an American announces he's going to change his pants, or an American experiences when an English man talks about going to the Norfolk Broads, or how he can't give up fags.

Now the question arises, if Dutch is so easy for an English speaker to learn, then why do so few English speakers in Holland actually speak Dutch? What I have only recently discovered is something that the Dutch people reading this will already know about only too well, and that is the organised movement to stop English speakers learning Dutch. For the benefit of English-speaking readers who don't know about this plot, I'll explain.

The major tactic is one of demoralisation. 'But Dutch is such an unimportant language!' they proclaim, if they hear that someone plans to learn it, or 'It's a terribly difficult language to learn' (as if they knew). A subtler approach is sarcasm. 'What good Dutch you speak!' they say, as you stutter out some half comprehensible anglicism, receiving the praise only because you pronounced the g's right.

The final tactic is ridicule. You go into a shop, and they suffer you to speak in Dutch and they reply in Dutch. But the moment you make a mistake, or fail to understand, they immediately continue in English, and nothing, nothing you say or do will get them back to their mother tongue.

But why this organised plan to prevent English speakers from learning Dutch, you ask. Well of course, if all the English speakers spoke Dutch, who then could the Dutch practise their English on?

For indeed, I can't imagine a country with more linguists than Holland: it's quite normal for a Dutch person to speak four languages, and watch TV programs from four countries. And which other country demands the ability to speak a foreign language as a condition for joining the police force? And where else can shop assistants, even outside the tourist areas, converse with you in English?

Living and working in Amsterdam has had one unexpected effect. Now when I go to an international conference, people say to me 'What good English you speak!' I still haven't decided whether to say 'Oh, I lived in England for awhile' or 'Yes, my mother's English you know.'

But the worst thing happened on holiday in Greece. I was speaking to an English man, and when I said I was on my way back to Amsterdam, he said 'Aha! I *thought* you weren't English!'

Open problems

All correspondence should be sent to the
editors of the
CWI Newsletter
*Centre for Mathematics and
Computer Science
Kruislaan 413
1098 SJ Amsterdam
The Netherlands*

1. The demographer's problem

An important problem in practical demography, concerning statistical estimation of a Markov process model, requires solution of the mathematical problem which is described below.

First we introduce some notation. For row vectors in $\mathbb{R}^p$ $(1 \leqslant p < \infty)$, '$\geqslant$' and '$>>$' denote componentwise $\geqslant$ and $>$ respectively. We denote by $\mathbf{0}$ and $\mathbf{1}$ the vectors all of whose components are 0 and 1 respectively. The unit simplex $\mathbb{S} \subset \mathbb{R}^p$ and its relative interior $\mathbb{S}^0$ are defined by

$$\mathbb{S} = \{x \geqslant \mathbf{0}\colon x\,\mathbf{1}^{\mathrm{T}} = 1\}$$

$$\mathbb{S}^0 = \{x >> \mathbf{0}\colon x\,\mathbf{1}^{\mathrm{T}} = 1\}.$$

The set of all $p \times p$ intensity matrices is

$$\mathcal{Q} = \{Q \in \mathbb{R}^{p \times p}\colon q_{ij} \geqslant 0 \ \ \forall i \neq j,\ Q\,\mathbf{1}^{\mathrm{T}} = \mathbf{0}^{\mathrm{T}}\}.$$

The problem to be solved is: given $\mu \in \mathbb{S}$ and $N \in \mathcal{Q}$ such that $\nu = \mu + \mathbf{1}N >> \mathbf{0}$, does there exist $l \in \mathbb{S}^0$ such that

$$l = \int_0^1 \mu e^{Qs}\,ds \quad \text{where} \quad Q = (\operatorname{diag} l)^{-1} N? \qquad (*)$$

If so is the solution unique? Do the iterations suggested by (*) converge?

Extensive numerical experimentation suggests that the answers to all three questions are positive. Using the *K-K-M* lemma and homotopy theory, the existence problem has been solved and some very partial results on uniqueness have been obtained [1]. In particular it is known that a solution to (*) does always exist and moreover if $\operatorname{rank}(N) = p - 1$ then $l \in \mathbb{S}^0$ solves (*) if and only if it also solves

$$\nu = \mu e^{Q} \quad \text{where} \quad Q = (\text{diag}\, l)^{-1} N. \qquad (^{**})$$

What about uniqueness and convergence?

Richard D. Gill

REFERENCE
1. R.D. GILL (1984). *On Estimating Transition Intensities of a Markov Process with Aggregate Data of a Certain Type,* Report MS-R8411, CWI Amsterdam.

2. ON FINITE QUATERNIONIC REFLECTION GROUPS

Let V be a vector space of finite dimension n over the field of complex (or real) numbers. A reflection on V is a linear nonidentity transformation fixing a linear subspace of dimension $n-1$ pointwise. A group of linear transformations on V is called a reflection group if it is generated by reflections. If G is a finite reflection group, then the stabilizer G_ν of any vector ν in V is again a reflection group in V. Proofs of this fact can be found in [1, p.139, ex.8] and [5]. In both proofs, the ring of polynomial functions on V invariant under G plays a crucial role. Therefore, they are no longer valid if the field of scalars is replaced by $\mathbb{H}$, the division ring of real quaternions. In view of the classification of finite quaternionic reflection groups, cf. [2], the question:

> Are all subgroups of finite reflection groups on a quaternionic vector space V fixing a vector again reflection groups?

can be answered by a case by case analysis. This has been done for all so-called imprimitive reflection groups and for all groups occurring in dimension $n \leqslant 3$ (by CUYPERS [3]). The question remains whether the statement is true for all G. If the answer is yes, a proof of this fact independent of the classification of finite quaternionic reflection groups would be useful in obtaining an elementary proof of this classification. (The present proof depends on the classification of all complex linear groups generated by elements fixing a linear subspace of dimension $n-2$ pointwise, cf. HUFFMAN-WALES [4].)

Arjeh M. Cohen

REFERENCES
1. N. BOURBAKI (1968). *Groupes et Algèbres de Lie, Chap. IV, V, VI,* Hermann, Paris.
2. A.M. COHEN (1980). Finite quaternionic reflection groups. *J. Algebra 64,* 293-324.
3. F.G.M.T. CUYPERS, private communication.

4. W.C. HUFFMAN, D.B. WALES (1977). Linear groups containing an involution with two eigenvalues -1. *J. Algebra 45,* 465-515.
5. R. STEINBERG (1964). Differential equations invariant under finite reflection groups. *Trans. Amer. Math. Soc. 112,* 392-400.

Abstracts

of Recent CWI Publications

When ordering any of the publications listed below please use the order form at the back of this issue.

CWI Tract 8. M.H. van Hoorn. *Algorithms and Approximations for Queueing Systems.*
AMS 60K25; 122 pp.

Abstract: In this monograph recursive computational schemes are given for the steady state probabilities and other performance measures for a wide class of single server and multi server queues. The ultimate goal is to obtain practically useful results and therefore the analysis is exact whenever possible and approximate whenever exact methods would lead to intractable results. Special attention has been paid to actual numerical calculations in order to check whether the proposed methods are indeed useful for practical purposes. Many numerical results and illustrations are given. In particular, the following models are analyzed: the $M/G/1$ queue and the $M/G/c$ queue with uniform or state dependent arrival rate, the $M^x/G/1$ queue with state dependent batch arrivals and the $H_2/G/1$ queue.

CWI Tract 9. C.P.J. Koymans. *Models of the Lambda Calculus.*
AMS 03B40, 68F20; 181 pp.

Abstract: In this book the semantics of the lambda calculus is studied. There are two conceptually different approaches to this subject. The first approach considers functions to be algorithms and gives rise to the notion of a *lambda algebra,* either by giving a direct interpretation of lambda terms (environment models) or by using the equivalent theory of strong combinatory logic. The second approach is set theoretical in that it identifies functions with their graphs. This leads to the notion of a *lambda model.* The unification of both methods using category theory is the main topic of this text. Both lambda algebras and lambda models can be defined naturally in this way. As an application of the category theoretic approach the theory of derived models is studied, analyzing the construction of a D_∞-like extensional lambda calculus model inside $P\omega$ as originally defined by Scott. The last chapter studies the properties of a special model, viz. Sanchis's hypergraph model. This turns out to be the first mathematical structure modelling combinatory logic, that cannot be expanded to a lambda model.

CWI Tract 10. C.G. van der Laan & N.M. Temme. *Calculation of Special Functions: The Gamma Function, The Exponential Integrals and Error-Like Functions.*
AMS 65D20, 65-04, 33-04; 231 pp.

Abstract: The main scope of this tract is to review and to discuss several aspects of implementations for the numerical computation of special functions. Especially three groups of functions are considered, namely those related to the Euler gamma function, exponential integrals and error functions. For each of these groups a systematic screening in the literature and several program libraries is performed. The information for each group includes: (1) definitions, analytic properties and fundamental formulas; (2) algorithms, implementations, error analysis, tabulated coefficients, testing. There is an introductory chapter on the literature and program libraries and a chapter on the theoretical background (error analysis, recurrence relations, continued fractions and generalized hypergeometric functions).

CWI Tract 11. N.M. van Dijk. *Controlled Markov Processes; Time-Discretization.*
AMS 60Jxx, J25/60/75, 93Exx, E20/25; 166 pp.
Abstract: This study investigates the method of time-discretization in order to approximate continuous-time controlled Markov processes and corresponding finite horizon cost functions. The approximation method is based on approximating time-evolution equations by one-step difference methods. For this an approximation lemma adopted from numerical analysis is presented. This lemma enables us to determine orders of convergence, which makes it of computational interest, as well as to deal with unbounded cost functions. We concentrate on approximations induced by discrete-time controlled Markov processes. As a result, by applying discrete-time dynamic programming we can compute the approximations. Much attention is paid to analyzing a specific discretization for controlled Markov jump and controlled diffusion processes.

CS-R8412. P.M.B. Vitányi. *Signal propagation delay, wire length distribution and the efficiency of VLSI circuits.*
AMS 68C25, 94C99; CR B.7.0, F.2.3; 11 pp.; **key words:** very large scale integrated circuits (VLSI), wafer scale integration, logarithmic signal propagation delay, electronic principles, driving long wires, wire aspect ratio, wire length distributions in VLSI layouts, Rent's Rule, layout area, computational complexity, efficiency.
Abstract: Using sound electronic principles, a signal propagation delay logarithmic in the length of a wire can be attained in VLSI circuits only if all wires in the layout have the same aspect ratio. This results in a penalty in surface area of the order of the square of the length of the wire. Thus, the global complexity of a VLSI circuit is affected. In particular, the complexity becomes very layout dependent. This effect will be truly pronounced in the emerging wafer scale integration technology. Simple theoretical considerations and experimental study of actual circuits have shown elsewhere that the wire length distribution $f(i)$ for the layout of integrated logic chips, in particular for VLSI, tend to satisfy $f(i) = c/i^{\lambda}(1 \leq i \leq L)$ and $f(i) \approx 0 (i > L)$. There are wire-length distributions for which the logarithmic delay assumption entails at least an exponential increase in area over the constant wire width assumption for any layout with that distribution. Consequently, the wires need to get so much longer to achieve logarithmic delay that the absolute propagation delay turns out to be not improved over an original linear or quadratic propagation delay. Taking into account also the fact that the wide wires have to be actually placed in a layout, the logarithmic delay requirement may in some cases not be implementable at all, apart from the fact that even if it could it would give no improvement in absolute time.

CS-R8414. P.M.B. Vitányi. *Circuit topology, signal propagation delay and the efficiency of VLSI circuits.*
AMS 68C25, 94C99; CR B.7.0, F.2.3; 18 pp.; **key words:** very large scale integrated circuits (VLSI), wafer scale integration, logarithmic signal propagation delay, electronic principles, driving long wires, wire aspect ratio, wire length distribution, circuit topology, layout area, computational complexity, efficiency, H-tree layout, Dictionary machine, Cube-Connected Cycles.

Abstract: Using sound electronic principles, a signal propagation delay logarithmic in the length of a wire can be attained in VLSI circuits only if all wires in the layout have the same aspect ratio. This results in a penalty in wire surface area of the order of the square of the length of the wire. Thus, the global complexity of a VLSI circuit is affected. In particular, the complexity becomes very layout dependent. This effect will be truly pronounced in the emerging wafer scale integration technology. There are circuit topologies with the same function (Dictionary machine, Fast Fourier Transform) such that a circuit topology which is optimal under one delay assumption is suboptimal under another. Under constant signal propagation delay, or logarithmic delay, systolic search trees or fast permutation networks of superior performance can be laid out if we assume constant width wires. However, under logarithmic signal propagation delay with the required constant aspect ratio for the wires the naïve Mesh layout is superior over every tree layout with respect to both Area and Period. Similarly, if the Fast Fourier Transform is implemented in this way, the naïve Mesh layout is superior over every layout for a fast permutation network like the Cube-Connected Cycles in Area, Area×Period and the Area×Execution Time. As a matter of independent interest, with a constant aspect ratio a for wires and using at most c layers, every layout for a complete N-node binary tree, and hence also the H-tree layout, takes Area $\Omega(N \log^{a/6c} N)$. With the wire aspect ratio and number of layers constant independent of N, it is impossible to layout a complete N-node binary tree using equal length wires.

CS-R8415. W.E. van Waning. *Engineering robot actions in a computer integrated manufacturing environment.*

AMS 86B20, 68G99, 68J10; CR D.2.6, I.2.9, J.1.6; 7 pp.; **key words:** computer integrated manufacturing (CIM), robotics, engineering design, design and organization of systems, programming environments.

Abstract: A model is presented according to which robot-actions and the activities in manufacturing cells can be designed. In this model, design-activities have three major aspects: specification, analysis and synthesis. Principles are then derived for the construction of programming systems for designing operations of robots and manufacturing cells. The specification describes an external environment (the device to be made and the tools to make it with). Given the outer environment and the knowledge specific to the discipline the engineer designs possible inner structures that serve as strategies specifying how to make the device in question. It is important that the engineer can express the designs symbolically. Finally, when synthesizing the process-structure the designed manufacturing process is matched against the external environment. The need is stressed for simulation environments so that it is possible to test the design thoroughly on the basis of actually observed sensor-data before the programs are taken into production.

CS-R8418. S.J. Mullender & A.S. Tanenbaum. *The design of a capability-based distributed operating system.*

AMS 68A05, 68B20; CR C.2.2, C.2.4, D.4.4, D.4.6; 19 pp.; **key words:** distributed operating systems, capabilities, connectionless protocols, transaction-oriented protocols, protection, accounting, file systems, service model.

Abstract: Fifth generation computer systems will use a large numbers of processors to achieve high performance. In this paper a capability-based operating system designed for this environment is discussed. Capability-based operating systems have traditionally required large, complex kernels to manage the use of capabilities. In our proposal, capability management is done entirely by user programs without giving up any of the protection aspects normally associated with capabilities. The basic idea is to use one-way functions and encryption to protect sensitive information. Various aspects of the proposed system are discussed.

CS-N8405. L.G.L.T. Meertens & S. Pemberton. *Description of B.*
AMS 69D41; 38 pp.; **key words:** Programming languages, *B*.
Abstract: *B* is a simple but powerful new programming language designed for use in personal computing. This report is intended as a reference book for the users of *B*, though it will also be useful for experienced programmers who want to learn *B*.

CS-N8407. L.J.M. Geurts. *Een kennismaking met de programmeertaal B*, Deel I.
AMS D.3.3, D.1.0, K.3.2; 85 pp.; **key words:** programming, programming languages, *B*.
This is a Dutch version of CS-N8402. (see Abstracts section of Newsletter no. 4).

CS-N8408. J.C. Ebergen. *On VLSI design.*
AMS 68C01, 68F05, 94C99; 8 pp.; **key words:** VLSI design, functional specification, regular expressions, layout of a circuit.
Abstract: Some of the problems in VLSI design are discussed. A VLSI design method is presented with which these problems may be tackled. An example is provided to illustrate some parts of the design method.

OS-R8409. M.W.P. Savelsbergh. *Local search in routing problems with time windows.*
AMS 69G11, 69G30, 69F13; 13 pp.; **key words:** vehicle routing problem, traveling salesman problem, time windows, local search, k-interchange, NP-completeness, computational complexity, heuristics.
Abstract: We develop local search algorithms for routing problems with time windows. The algorithms presented are based on the k-interchange concept. The presence of time windows introduces feasibility constraints, the checking of which normally requires $O(N)$ time. Our method reduces this checking effort to $O(1)$ time. We also consider the problem of finding initial solutions. A complexity result is given and an insertion heuristic is described.

OS-R8410. E.A. van Doorn. *A note on equivalent random theory.*
AMS 60K30, 90B22; 4 pp.; **key words:** teletraffic theory, equivalent random theory, overflow traffic, peakedness factor.
Abstract: The purpose of this note is to provide proofs for two fundamental results in equivalent random theory that are generally accepted as valid, but for which no proofs are available in the literature.

NM-R8408. P.J. van der Houwen & B.P. Sommeijer. *High order difference schemes with reduced dispersion for hyperbolic differential equations.*
AMS 65M20, 76B15; 25 pp.; **key words:** hyperbolic equations, difference schemes, Runge-Kutta methods, dispersion.
Abstract: We investigate difference schemes for systems of first order hyperbolic differential equations in two space dimensions, possessing the following characteristics: (i) The spatial discretizations are fourth order accurate. (ii) The time discretization is of explicit Runge-Kutta type and is also fourth order accurate. (iii) The scaled stability boundary is approximately $\sqrt{2}/2$. (iv) The weights in the space discretizations and the Runge-Kutta parameters can be adapted so as to reduce the dispersion of the dominant Fourier components in the solution.

This method is illustrated by applying it to the shallow water equations simulating the motion of water in a shallow sea due to tidal forces. Since in such problems the dominant frequencies in the solution are known in advance, the method can take full advantage of the possibility of tuning the various parameters to these dominant frequencies.

NM-R8409. P.J. van der Houwen & J.G. Blom. *Stability results for discrete Volterra equations: Numerical experiments.*
AMS 65R20; 12 pp.; **key words:** numerical analysis, Volterra integral equations, stability.
Abstract: In this paper we formulate a local stability criterion for linear multistep discretizations of first- and second-kind Volterra integral equations with finitely decomposable kernel. In a large number of numerical experiments this criterion is tested. We did not find examples with unstable behaviour while the stability criterion predicted stability. However, we found several examples with stable behaviour while the stability criterion predicted instability. A possible explanation may be the fact that the stability criterion is independent of the decomposition of the kernel, that is, it holds for the most ill-conditioned decomposition and consequently it may be rather pessimistic.

NM-R8410. P.J. van der Houwen, B.P. Sommeijer & C.T.H. Baker. *On the stability of predictor-corrector methods for parabolic equations with delay.*
AMS 65Q05, 65M20, 35R10; 16 pp.; **key words:** parabolic equations, delay equations, predictor-corrector methods.
Abstract: Diffusion problems where the current state depends upon an earlier one give rise to parabolic equations with delay. The efficient numerical solution of classical parabolic equations can be accomplished via methods for stiff differential equations. One such class are predictor-corrector-type methods with extended real stability intervals and with reduced storage requirements. Analogous methods for equations with delay are proposed and analyzed here. Numerical experiments which illustrate the theoretical results are reported.

NM-R8411. J.G. Verwer. *On the shift parameter in the backward beam method for parabolic problems for preceding times.*
AMS 65M30, 65M20, 65L10; CR 5.17; 9 pp.; **key words:** backward heat problems, ill-posed problems, numerical analysis, boundary value methods, backward beam method.
Abstract: We consider the backward beam method of Buzbee & Carasso *(Math. Comp.* **27** (1973), 237-267) for the numerical computation of parabolic problems for preceding times. The performance of this method is strongly influenced by the choice of a spectral shift parameter. Using logarithmic convexity arguments Buzbee & Carasso derived an expression for the optimal value for linear problems. The main concern of this paper is to illustrate that this expression can also be found and explained via the numerical stability analysis of the forward and backward recurrence involved.

NM-R8412. A.M. Odlyzko & H.J.J. te Riele. *Disproof of the Mertens conjecture.*
AMS 10A20, 10H05, 65E05, 06C10; CR 5.12; 18 pp.; **key words:** Mertens conjecture, Riemann hypothesis, Lattice basis reduction algorithm, multiple precision computation, zeros of the Riemann zeta function.
Abstract: The Mertens conjecture states that $|M(x)| < x^{1/2}$ for all $x > 1$, where

$$M(x) = \sum_{n \leq x} \mu(n)$$

and $\mu(n)$ is the Möbius function. This conjecture has attracted a substantial amount of interest in its almost 100 years of existence because its truth was known to imply the truth of the Riemann

hypothesis. This paper disproves the Mertens conjecture by showing that

$$\limsup_{n \to \infty} M(x)x^{-1/2} > 1.06.$$

The disproof relies on extensive computations with the zeros of the zeta function, and does not provide an explicit counterexample.

NM-R8413. W.H. Hundsdorfer & M.N. Spijker. *On the algebraic equations in implicit Runge-Kutta methods.*

AMS 65L05, 47H15, 65H10; 13 pp.; **key words:** numerical analysis, stiff initial value problems, implicit Runge-Kutta methods, nonlinear algebraic equations, stability.

Abstract: This paper is concerned with the system of (nonlinear) algebraic equations which arise in the application of implicit Runge-Kutta methods to stiff initial value problems. Without making the classical assumption that the stepsize $h > 0$ is small, we derive transparent conditions on the method that guarantee existence and uniqueness of solutions to the equations. Besides, we discuss the sensitivity of the Runge-Kutta procedure with respect to perturbations in the algebraic equations.

MS--R8411. R.D. Gill. *On estimating transition intensities of a Markov process with aggregate data of a certain type.*

AMS 62M05, 62Pxx; 12 pp.; **key words:** Markov process, aggregate data, multidimensional mathematical demography, multistate life-table, occurrence-exposure rate, fixed-point theorem, degree theory.

Abstract: In demography finite-state-space time-homogeneous Markov processes are often used, explicitly or implicitly, to model the movement of individuals between various states (e.g. studies of marital formation and dissolution or of interregional migration). However, the fact that data is often only available at certain levels of aggregation, preventing a simple and exact statistical analysis, has caused much confusion and has even impeded the adoption of probabilistic modelling and statistical analysis. In this paper we consider one specific form of aggregate data and propose a new method of estimation of the underlying Markov process. Some preliminary results on the properties of this method are given and some open problems are discussed.

MS-R8412. H.C.P. Berbee. *Convergence rates in the strong law for bounded mixing sequences.*

AMS 60F15, 60G10, 60K05; 16 pp.; **key words:** mixing, Marcinkiewicz-Zygmund strong law, coupling, moment inequality, renewal theory.

Abstract: Speed of convergence is studied in the Marcinkiewicz-Zygmund strong law for partial sums of bounded dependent random variables under conditions on their mixing rate. Though α-mixing is also considered, the most interesting result concerns absolutely regular sequences. The results are applied to renewal theory to show estimates obtained there by coupling are best possible. Another application sharpens a result for averaging a function along a random walk.

AM-R8410. B. Dijkhuis. *On the propagation speed in relativistic quantum mechanics.*

AMS 81M05, 81D05, 47B47; 4 pp.; **key words:** propagation speed in relativistic quantum mechanics, local commutativity, superluminal velocity.

Abstract: A new definition of propagation speed is proposed. Assuming that there is a maximal speed, we derive an operator condition that resembles the condition of local commutativity in quantum field theory. The relativistic energy-momentum relation implies that the maximal speed is not smaller than the speed of light. We discuss an example that shows a superluminal propagation speed.

AM-R8411. N.M. Temme. *A class of polynomials related to those of Laguerre.*
AMS 33A65, 41A60; 6 pp.; **key words:** Laguerre polynomials, asymptotic expansion.

Abstract: We consider a class of polynomials, defined by $l_n(x) = (-1)^n L_n^{x-n}(x)$, which were introduced by F.G. Tricomi. We explain the role of the polynomials in asymptotics, especially in uniform expansions of a Laplace-type integral. Moreover, an asymptotic expansion of $l_n(x)$ is given for $n \to \infty$ which refines results of Tricomi and Berg.

AM-R8412. N.M. Temme. *Uniform asymptotic expansions of integrals.*
AMS 41A60, 33-xx, 30E15; 13 pp.; **key words:** asymptotic expansions of integrals, uniform asymptotic expansions, special functions.

Abstract: The purpose of the paper is to give an account of several aspects of uniform asymptotic expansions of integrals. We given examples of standard forms, the role of critical points and methods for constructing the expansions.

AM-R8413. H.A. Lauwerier. *Dynamical systems and numerical integration.*
AMS 58F14, 65D30, 39A10; 25 pp.; **key words:** dynamical systems, numerical integration, difference equations.

Abstract: A few schemes for the numerical integration of ordinary differential equations are considered as discrete dynamical systems. The properties of those systems centered around the Poincaré-Birkhoff theorem and the Kolmogorov-Arnold-Moser (KAM) theorem may give a deeper understanding of the global behaviour of integration schemes and may explain the occurrence of unwanted phenomena such as 'chaotic' oscillations. This approach is of wider generality than the usual technique of Taylor expansions, a technique which is not always justified and may even be wrong.

AM-R8414. H.J.A.M. Heijmans. *The dynamical behaviour of the age-size-distribution of a cell population.*
AMS 92A15; 25 pp.; **key words:** age-size-distribution, integration along characteristics, abstract renewal equation, Laplace transform, operator-valued function, positive operator, non-supporting operator, dominant singularity, renewal theorem.

Abstract: We study the model proposed by Bell and Anderson describing the dynamics of a proliferating cell population. This model assumes that the individual's behaviour is completely determined by its age and size. By the method of integration along characteristics the problem is reduced to a renewal type integral equation. Using Laplace transform techniques and results from positive operator theory we can describe the large time behaviour of the solution, if we impose a condition on the growth rate.

AM-N8403. H.A. Lauwerier. *The blooming tree of Pythagoras.*
AMS 51-01, 51-04; 14 pp.; **key words:** Pythagoras tree.

Abstract: A description is given of the so-called Pythagoras tree and how it can be drawn by means of a simple computer program. Apart from the geometrical construction an approach is given in which complex numbers and binary representations of numbers is used.

PM-R8407. M. Hazewinkel. *On positive vectors, positive matrices and the specialization ordering.*
AMS 06A10, 15A48, 15A51; 7 pp.; **key words:** specialization order, nonnegative matrices, majorization.

Abstract: A brief introductory discussion is given of the specialization partial ordering for positive

vectors in connection with the positive rank of nonnegative matrices.

PM-R8408. A. del Junco & D.J. Rudolph. *On ergodic actions whose self-joinings are graphs.*
AMS 28D05, 28D15; 54 pp.; **key words:** ergodic group actions, joinings, factors, group extensions.
Abstract: We call an ergodic measure-preserving action of a locally compact group G on a probability space *simple* if every ergodic joining of it to itself is either a product measure or is supported on a graph, and a similar condition holds for multiple self-joinings. This generalizes Rudolph's notion of minimal self-joinings and Veech's property S. Main results: the joining of a simple action with an arbitrary ergodic action can be explicitly described. A weakly-mixing group extension of an action with minimal self-joinings is simple. The action of a closed, normal, co-compact subgroup in a weakly-mixing simple action is again simple. Some corollaries: two simple actions with no common factors are disjoint. The time-one flow of a weakly-mixing flow with minimal self-joinings is prime. Distinct positive times in a $\mathbb{Z}$-action with minimal self-joinings are disjoint.

PM-R8409. E.P. van den Ban. *Invariant differential operators on a semisimple symmetric space and finite multiplicities in a Plancherel formula.*
AMS 22E30, 22E46, 43A85; 11 pp.; **key words:** semisimple symmetric spaces, Plancherel formula, discrete series, invariant differential operators.
Abstract: We investigate some properties of the algebra $\mathbb{D}(G/H)$ of invariant differential operators on a semisimple symmetric space G/H. Our main results are that the action of $\mathbb{D}(G/H)$ diagonalizes over the discrete part of $L^2(G/H)$, and that the irreducible constituents of an abstract Plancherel formula for $L^2(G/H)$ occur with finite multiplicities. In particular this implies that discrete series representations occur with finite multiplicities in $L^2(G/H)$.

PM-R8410. E.P. van den Ban. *Asymptotic behaviour of matrix coefficients related to reductive symmetric spaces.*
AMS 22E30, 22E46, 43A85; 76 pp.; **key words:** reductive symmetric space, matrix coefficient, asymptotic behaviour, Schwartz space.
Abstract: We study the asymptotic behaviour of K-finite H-invariant matrix coefficients related to a reductive symmetric space G/H. In all directions to infinity this behaviour is described by absolutely converging series expansions similar to those in the group case. A generalization of Harish-Chandra's Schwartz space is introduced.

PM-R8411. M. Hazewinkel. *Experimental mathematics.*
AMS 00A05, 00A25, 58F03, 82F03, 35Q03; 38 pp.; **key words:** experimental mathematics.
Abstract: Experimental mathematics in this paper is understood to mean the use of a computer for doing mathematical experiments. For instance experiments designed to get the first glimmer of an idea how to tackle a given set of problems or experiments to indicate where to look for counterexamples or to make the conjecture more precise. This is rapidly becoming a major area of research and may well develop into a semi-separate discipline like computational fluid dynamics or statistics.

PM-R8412. T.H. Koornwinder. *Squares of Gegenbauer polynomials and Milin type inequalities.*
AMS 30C50, 33A30, 33A65; 4 pp.; **key words:** Bieberbach conjecture, Milin conjecture, positive ${}_3F_2$ hypergeometric functions, squares of Gegenbauer polynomials.

Abstract: De Branges, in his proof of the Bieberbach conjecture, was led to a specific solution with monotonicity properties of a certain linear system of differential equations. We present other solutions with similar monotonicity properties, the derivatives of their coordinates being multiples of squares of Gegenbauer polynomials. De Branges' solution is a nonnegative linear combination of our solutions. As a corollary we obtain Milin type inequalities for logarithmic power series coefficients of univalent analytic functions on the unit disk which are sharper than the Milin conjecture.

PM-R8413. E. Badertscher. *Harmonic analysis and Radon transforms on pencils of geodesics.*
AMS 51M10, 33A75, 43A32, 43A90; 21 pp.; **key words:** classical geometries, pencils of geodesics, spherical functions, *c*-functions, Jacobi functions, spherical Fourier transform, product formulas, integral representations, Radon transforms, fractional integral transforms, convolution products.

Abstract: We introduce pencils of geodesics as generalized points in classical geometries X. We generalize the spherical harmonic analysis on X to pencils (in particular we consider spherical functions and spherical Fourier transforms on pencils). By means of 'Radon transforms' (i.e. by changing the invariance type of a function through integration) we can relate the theories of different pencils. By evaluating the Radon transforms of spherical functions we get various product formulas. In the interesting case that $X = \mathbb{H}^n$ (hyperbolic n-space) we express everything explicitly. The spherical functions in particular can be expressed by Jacobi functions, the Radon transforms can be reduced to fractional integral transforms. By a Radon transform we also transfer the convolution structure from K-invariant functions on $\mathbb{H}^n$ to H-invariant functions on $\mathbb{H}^n (K = SO(n), H = SO_0(1,n-1))$.

PM-N8402. M. Hazewinkel. *On mathematical control engineering.*
AMS 93-02; 10 pp.; **key words:** mathematical control and system theory, filtering.

Abstract: An introductory account is given of the mathematical problems arising in electrical and control engineering.

CWI Activities

Winter 1984

With each activity we mention its frequency and (between parentheses) a contact person at CWI. Sometimes some additional information is supplied, such as the location if the activity will not take place at CWI.

Study group on Analysis on Lie groups. Joint with University of Leiden. Biweekly. (E.P. van den Ban)

Seminar on Algebra and Geometry. Coxeter Groups and Combinatorics. Biweekly. (A.E. Brouwer)

Study group on Cryptography. Biweekly. (J.H. Evertse)

Colloquium 'STZ' on System Theory, Applied and Pure Mathematics. Twice a month. (J. de Vries)

Study group 'Biomathematics'. Lectures by visitors or members of the group. Joint with University of Leiden. (J. Grasman)

Study group 'Nonlinear Analysis'. Lectures by visitors or members of the group. Joint with University of Leiden. (O. Diekmann)

Progress Meetings of the Applied Mathematics Department. New results and open problems in biomathematics, mathematical physics and analysis. Weekly. (N.M. Temme)

National Study Group on Statistical Mechanics. Joint with Technological University of Delft, Universities of Leiden and Groningen. Monthly. University of Amsterdam. (H. Berbee)

Progress meetings of the Mathematical Statistics Department. New results in research and consultation projects. Monthly. (R.D. Gill)

Lunteren Meeting on Stochastics. 12,13,14 November 1984 at 'De Blije Werelt', Lunteren. Invited speakers:
M.L. Eaton (University of Minnesota, USA), S. Kakutani (Yale, New Haven, Connecticut, USA), D.W. Müller (University of Heidelberg, West Germany), J. Pfanzagl (University of Cologne, West Germany). H. Rootzén (University of Copenhagen, Denmark), J.E. Yukich (MIT, temporarily

Strasburg). Joint with Dutch Mathematical Society and Dutch Statistical Society. (R. Helmers)

Seminar on Probability Inequalities and Related Topics, given by M.L. Eaton. Joint with University of Amsterdam (and held there). Weekly. (R.D. Gill)

Tenth Conference on the Mathematics of Operations Research. 9,10,11 January 1985 at Lunteren. Invited lecturers are:
J.B. Orlin (Cambridge, USA), M.J.D. Powell (Cambridge, UK), G.P. Prastacos (Athens, Greece), R.R. Weber (Cambridge, UK). (E.A. van Doorn)

Progress meetings on Combinatorial Optimization. Biweekly. (J.K. Lenstra)

System Theory Days. Irregular. (J.H. van Schuppen)

Study group on System Theory. Biweekly. (J.H. van Schuppen)

National colloquium on Optimization. Irregular. (J.K. Lenstra)

Study group on Differential and Integral Equations. Lectures by visitors or group members. Biweekly. (H.J.J. te Riele)

Study group Numerical Flow Dynamics. Lectures by group members. Every Wednesday. (J.G. Verwer)

Study group Hyperbolic systems. Every Wednesday. (P.W. Hemker)

Progress meetings on Numerical Mathematics. Weekly. (H.J.J. te Riele)

Seminar National Concurrency Project. Joint with Universities of Leiden, Utrecht, Nijmegen and Amsterdam. 22 February, 22 March and 24 May. (J.W. de Bakker)

National Study Group 'Concurrency'. Joint with Universities of Leiden, Utrecht, Nijmegen and Amsterdam. 18 January, 8 February, 8 March and 5 April. University of Utrecht. (J.W. de Bakker)

Post-academic course on Modern Techniques in Software Engineering. 7,8 21 and 22 February. (J.C. van Vliet)

Post-academic course on *B*. 7 January - 9 May. Twice a week. (L. Geurts)

Study group on Graphics Standards. Monthly. (M. Bakker)

Study group 'Dialogue programming'. (P.J.W. ten Hagen)

Visitors to CWI from Abroad

A. Bruen (The University of Western Ontario, London, Canada) 30 October. H. Brunner (University of Fribourg, Switzerland) 10-12 December. F. Calogero (University of Rome, Italy) 26 September - 3 October. Cheng Kan (Academia Sinica, Beijing, China) 25 November - 7 December. P. Cockshott (University of Glasgow, Scotland) 2-4 October. M.L. Eaton (University of Minnesota, USA) September 1984 - August 1985. C. van Eeden (University of Montreal, Canada) September 1984 - August 1985. J. Grizzle (University of Texas, Austin, USA) 5-26 November. M.R. Guevara (McGill University, Montreal, Canada) 27 November. Hsu Guang-hui (Academia Sinica, Beijing, China) 25 November - 7 December. R. Marumbar (University of Columbia, USA) 3 December. M. Mimura (University of Hiroshima, Japan) 29 October - 2 November. J. Saxl (University of Cambridge, UK) 26 November. W. Schappacher (University of Graz, Austria) 12 December. D. Schroeer (University of North Carolina, USA) 25 September. He Shi (Academia Sinica, Beijing, China) 19-21 November. A. Strasburger (University of Warsaw, Poland) 14 December. R. Wong (University of Manitoba, Winnipeg, Canada) 7-8 October.

Order Form for CWI Publications

Centre for Mathematics and Computer Science
Kruislaan 413
1098 SJ Amsterdam
The Netherlands

☐ Please send the publications marked below on an exchange basis
☐ Please send the publications marked below with an invoice

	Publication code	Price per copy	Number of copies wanted
☐	CWI Tract 8 *)	Dfl. 17.90	....
☐	CWI Tract 9 *)	26.20	....
☐	CWI Tract 10 *)	33.30	....
☐	CWI Tract 11 *)	23.80	....
☐	CS-R8412	3.70	....
☐	CS-R8414	3.70	....
☐	CS-R8415	3.70	....
☐	CS-R8418	3.70	....
☐	CS-N8405	6.--	....
☐	CS-N8407	11.90	....
☐	CS-N8408	3.70	....
☐	OS-R8409	3.70	....
☐	OS-R8410	3.70	....
☐	NM-R8408	3.70	....
☐	NM-R8409	3.70	....
☐	NM-R8410	3.70	....
☐	NM-R8411	3.70	....
☐	NM-R8412	3.70	....

*) not available on exchange

	Publication code	Price per copy	Number of copies wanted
☐	NM-R8413	3.70	....
☐	MS-R8411	3.70	....
☐	MS-R8412	3.70	....
☐	AM-R8410	3.70	....
☐	AM-R8411	3.70	....
☐	AM-R8412	3.70	....
☐	AM-R8413	3.70	....
☐	AM-R8414	3.70	....
☐	AM-N8403	3.70	....
☐	PM-R8407	3.70	....
☐	PM-R8408	8.40	....
☐	PM-R8409	3.70	....
☐	PM-R8410	10.80	....
☐	PM-R8411	6.--	....
☐	PM-R8412	3.70	....
☐	PM-R8413	3.70	....
☐	PM-N8402	3.70	....

If you wish to order any of the above publications please tick the appropriate boxes and return the completed form to our Sales Department.
Don't forget to add your name and address !
Prices are given in Dutch guilders and are subject to change without notice. Foreign payments are subject to a surcharge per remittance to cover bank, postal and handling charges.

Name ....

Street ....

City ....

Country ....

Contents