Astérisque

AST

Journées arithmétiques de Genève - 9-13 septembre 1991 : Pages préliminaires

Astérisque, tome 209 (1992), p. 1-16

<http://www.numdam.org/item?id=AST_1992__209__1_0>

209 ASTÉRISQUE

1992

JOURNÉES ARITHMÉTIQUES DE GENÈVE

9 - 13 septembre 1991

D.F. CORAY, Y.-F. S. PÉTERMANN, éditeurs

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

A.M.S. Subjects Classification (par article, dans l'ordre de la table des matières) :
• 11D61 (11D57 - 11E76 - 11R09) • 11G (14G) • 11M06 (11M41) • 20G30 (20H05) •11G40 • 11G05 • 11T06 (11P05) • 11H55 • 11J91 • 11C20 (15A36) • 11R33 (14L30) • 11B75 •11G35 (14G25) • 11R34 • 11S20 • 11N13 (11M26) • 11K55 • 11F70 • 11T71 • 11N37 • 11E25 (11E20-11P21) • 22E40 (11E12 - 20H15) • 11J91 • 11A55 (11B25 - 11D09) • 11G25 •

Préface

Les dix-septièmes Journées Arithmétiques ont rassemblé à Genève 213 mathématiciens de 26 pays, du 9 au 13 septembre 1991. Treize conférenciers ont présenté des exposés généraux accessibles à l'ensemble du public; près d'une centaine de communications plus spécialisées ont été réparties en quatre sessions parallèles. Le présent volume contient les textes de quelques-uns de ces exposés.

Ce congrès s'est déroulé sous le patronage de la Société Mathématique Suisse. Il a en outre bénéficié du soutien des institutions suivantes:
Université de Genève; Fonds national suisse de la recherche scientifique; C.N.R.S.; Académie suisse des sciences naturelles; Société Académique (Genève); Etat de Genève; Etat du Valais; 3ème Cycle romand de mathématiques; Association Jan Hus (Lausanne); Caran d'Ache S.A. (Genève); I.B.M. (Suisse) S.A.

En ce qui concerne le présent volume, nous tenons à exprimer notre gratitude aux quelque 40 rapporteurs anonymes, qui avec efficacité et rapidité ont abattu un travail considérable. Leurs remarques et critiques ont formé une contribution essentielle à la composition, la forme, et parfois le fond de la version définitive de ces comptes rendus.

Daniel Coray et Y.-F. S. Pétermann

JA 91 *Genève*

Table des Matières

Liste des participants

Montserrat ALSINA I AUBACH	Universitat de Barcelona
Hédi AMARA	Université de Tunis
Francesco AMOROSO	Università di Padova
Jannis A. ANTONIADIS	University of Crete
Gabriel ARCHINARD	Université de Genève
Angela ARENAS	Universitat de Barcelona
Maurice ARRIGONI	Université de Besançon
Roland BACHER	Université de Genève
Christine BACHOC	Université de Bordeaux I
U. BALAKRISHNAN	Tata Institute, Bombay
Daniel BARSKY	Université Paris 13
Victor V. BATYREV	Univ. Gesamthochschule Essen
Abdelmejid BAYAD	Université de Bordeaux I
Eva BAYER	Université de Besançon
Anne-Marie BERGÉ	Université de Bordeaux I
Dominique BERNARDI	Université Paris 6
Valérie BERTHÉ	E. N. S. / Univ. Paris 11
Marie-José BERTIN	Université Paris 6
Daniel BERTRAND	Université Paris 6
Gautami BHOWMIK	Jesus & Mary College of New Delhi
Hervé BILLARD	Université Paris 7
Maria Isabel BINIMELIS BASSA	Universitat de Barcelona
Laure BLASCO	Université de Strasbourg
Jacek BOCHŃAK	Vrije Universiteit Amsterdam
Sigrid BÖGE	Universität Heidelberg
Xavier BOICHUT	Université de Paris-Nord
Jean-Pierre BOREL	Université de Limoges
Jan BRINKHUIS	Erasmus University, Rotterdam

Jerzy BROWKIN	Warsaw University
Jörg BRÜDERN	Universität Göttingen
Juliusz BRZEZIŃSKI	Chalmers Univ. of Technology, Göteborg
Peter BUNDSCHUH	Universität zu Köln
Catalina CALDERÓN GARCÍA	Universidad del País Vasco
Philippe CASSOU-NOGUÈS	Université de Bordeaux I
Pierrette CASSOU-NOGUÈS	Université de Bordeaux I
Emmanuel CATELAND	Université de Bordeaux I
Gongliang CHEN	Université de Saint-Étienne
Habib CHÉRIF	Université de Bordeaux I
V. I. CHERNOUSOV	Acad. of Sciences B. S. S. R., Minsk
Henri COHEN	Université de Bordeaux I
Mark David COLEMAN	University of Manchester
Jean-Louis COLLIOT-THÉLÈNE	C. N. R. S. / Université de Paris-Sud
J. Brian CONREY	Oklahoma State University
Daniel CORAY	Université de Genève
Capi CORRALES	Universidad Complutense de Madrid
Anne CORTELLA	Université de Besançon
Teresa DE DIEGO	Université Paris 7
Jean-Marie DE KONINCK	Université Laval
Ilaria DEL CORSO	Scuola Normale Superiore di Pisa
J. R. DELGADO	Universidad Complutense de Madrid
Jean-Marie DELLEY	Université de Genève
Laurent DENIS	Université Paris 6
Jean-Guy DIAZ	Université de Saint-Étienne
Francisco J. DIAZ Y DIAZ	Université de Bordeaux I
Jean-Claude DOUAI	Université Paris 6
François DRESS	Université de Bordeaux I
Eugène DUBOIS	Université de Caen
René DUSSAUD	Chambéry
Roberto DVORNICICH	Università di Pisa
Shalom ELIAHOU	Université de Genève
Carsten ELSNER	Universität Hannover
Michel EMSALEM	Université Paris 7
Boas EREZ	Harvard University
Valérie FLAMMANG	Université de Metz
Vincent FLECKINGER	Université de Besançon
Francois FOUCAULT	Caen

Étienne FOUVRY	Université de Paris-Sud
Günther FREI	E. T. H. Zürich
Gregory FREIMAN	Tel Aviv University
Jean FRESNEL	Université de Bordeaux I
Carlo GASBARRI	Università di Roma "La Sapienza"
Marie-Laure GAUNET	Université de Caen
Jan VAN GEEL	Rijksuniversiteit Gent
Roland GILLARD	Université de Grenoble I
Catherine GOLDSTEIN	Université de Paris-Sud
Marc GRANDET	Université de Toulouse
Georges GRAS	Université de Besançon
Marie-Nicole GRAS	Université de Besançon
Barry W. GREEN	Universität Heidelberg
Cornelius GREITHER	Universität München
Kálmán GYŐRY	University of Debrecen
Franz HALTER-KOCH	Karl-Franzens-Universität Graz
Jaroslav HANČL	University of Ostrava
David HARARI	École Normale Supérieure
G. N. TEN HAVE	University of Leiden
Marc HINDRY	Université Paris 7
Pascal HUBERT	E. N. S. Lyon
Werner HÜRLIMANN	Winterthur
Marc HUTTNER	Université de Lille
Aleksandar IVIĆ	University of Belgrade
Uwe JANNSEN	Universität zu Köln
Piotr JAWORSKI	Warsaw University
Arnaud JEHANNE	Université de Bordeaux I
Wolfgang JENKNER	Karl-Franzens-Universität Graz
Henri JORIS	Université de Lausanne
Jerzy KACZOROWSKI	Adam Mickiewicz University, Poznań
Bruno KAHN	Université Paris 7
Shigeru KANEMITSU	Kinki University in Kyushu
Michel KERVAIRE	Université de Genève
John KNOPFMACHER	University of the Witwatersrand
Michel KOSKAS	Université Paris 6 / E.N.S.
B. È. KUNYAVSKIĬ	Saratov Inst. for Mech. in Agriculture
Gilles LACHAUD	C. N. R. S. Marseille
Erich LAMPRECHT	Universität des Saarlandes

Joan-C. LARIO	Universitat politècnica de Catalunya
Miroslav LAŠŠÁK	Universitas Comenianae, Bratislava
Michel LAURENT	Université Paris 6 / C.N.R.S.
Odile LECACHEUX	Université Paris 6
Günter LETTL	Karl-Franzens-Universität Graz
Armin LEUTBECHER	Technische Universität München
Lutz LUCHT	Technische Universität Clausthal
Maria Dolors MAGRET PLANAS	Universitat politècnica de Catalunya
Yu. I. MANIN	Steklov Institute, Moscow
Constantin MANOIL	Université de Genève
František MARKO	Slovak Academy of Sciences, Bratislava
Roman MARSZALEK	Wroclaw University
Jacques MARTINET	Université de Bordeaux I
Richard MASSY	Université de Valenciennes
Roland MATTHES	Gesamthochschule Kassel
Marcin MAZUR	Warsaw University
Hartmut MENZER	Friedrich-Schiller Universität Jena
Armel MERCIER	Université du Québec à Chicoutimi
Tom MEURMAN	University of Turku
Philippe MICHEL	Université de Paris-Sud
Maurice MIGNOTTE	Université de Strasbourg
Jiří MOČKOŘ	University of Ostrava
Jesús MONTES PERAL	Universitat de Barcelona
Pieter MOREE	University of Leiden
Baruch ben Zelik MOROZ	Max-Planck Institut für Mathematik
Yoichi MOTOHASHI	Nihon University
M. Ram MURTY	McGill University
Kenji NAGASAKA	Hosei University
Shoichi NAKAJIMA	Tokyo University
Thong NGUYEN QUANG DO	Université de Besançon
Jean-Louis NICOLAS	Université de Lyon I
Gerhard NIKLASCH	Technische Universität München
Břetislav NOVÁK	Charles University, Prague
Michel OLIVIER	Université de Bordeaux I
Michel OUELLET	Collège de Sainte-Foy
PATHIAUX-DELEFOSSE	Université Paris 6
Isabelle PAYS	Université de Mons-Hainaut
Roger PAYSANT-LE-ROUX	Université de Caen

Marc PERRET	Université Aix-Marseille II
Bernadette PERRIN-RIOU	Université Paris 6
Y-F. S. PÉTERMANN	Université de Genève
Meinhard PETERS	Universität Münster
Emmanuel PEYRE	École Normale Supérieure
Albrecht PFISTER	Universität Mainz
Thanases PHEIDAS	University of Crete
Georges PHILIBERT	Université de Saint-Étienne
Constantin PIRON	Université de Genève
Carl POMERANCE	University of Georgia
Florian POP	Universität Heidelberg
Dimitrios POULAKIS	Université de Thessalonique
Heinz-Georg QUEBBEMANN	Universität Oldenburg
Jacques QUEYRUT	Université de Bordeaux I
Adolfo QUIRÓS	Universidad Autónoma de Madrid
K. RAMACHANDRA	Tata Institute, Bombay
Olivier RAMARÉ	Université de Bordeaux I
Philippe RAMBOUR	Université de Paris-Sud
A. S. RAPINCHUK	Acad. of Sciences B. S. S. R., Minsk
Winfried RECKNAGEL	Fachhochschule München
Georges RHIN	Université de Metz
Marcello ROBBIANI	E. T. H. Zürich
Guy ROBIN	Université de Limoges
José-Luis RUIZ	Universitat politècnica de Catalunya
Nicolas SABY	Université de Grenoble I
Éric SAIAS	Université Paris 6
Jürgen W. SANDER	Universität Hannover
Philippe SATGÉ	Université de Caen
Fumihiro SATO	Rikkyo University
Volker SCHÄFFER	Universität Hannover
Rudolf SCHARLAU	Universität Bielefeld
Andrzej SCHINZEL	P. A. N., Warsaw
Anthony J. SCHOLL	University of Durham
Rainer SCHULZE-PILLOT	Universität Bielefeld
Jean-Pierre SERRE	Collège de France
Hironori SHIGA	Chiba University
Tetsuji SHIODA	Rikkyo University
François SIGRIST	Université de Neuchâtel

Mariusz SKALBA	Warsaw University
A. N. SKOROBOGATOV	Acad. of Sciences U. S. S. R., Moscow
Abdelhakim SMATI	Université de Limoges
Bouchaïb SODAÏGUI	Université de Valenciennes
David SOLOMON	Université de Bordeaux I
S. SRINIVASAN	Tata Institute, Bombay
John STEINIG	Université de Genève
Peter STEVENHAGEN	Université de Besançon
Noriyuki SUWA	Tokyo Denki University
Sir Peter SWINNERTON-DYER	Cambridge University
Bogdan SZYDLO	Adam Mickiewicz University, Poznań
Jean-Daniel THÉROND	Université de Montpellier
Philippe TOFFIN	Université de Caen
George TOMANOV	Bulgarian Academy of Sciences
Chédly TOUIBI	Université de Tunis
David TRANAH	Cambridge University
Artur TRAVESA	Universitat de Barcelona
Yuri TSCHINKEL	M. I. T.
M. A. TSFASMAN	Acad. of Sciences U. S. S. R., Moscow
Stephen V. ULLOM	University of Illinois at Urbana
Keijo VÄÄNÄNEN	University of Oulu
Michel VÉRANT	Université de Besançon
VERGER-GAUGRY	Université de Grenoble I
Nuria VILA	Universitat de Barcelona
Carlo VIOLA	Università di Pisa
Albert VIOLANT I HOLZ	Universitat de Barcelona
S. G. VLĂDUŢ	Acad. of Sciences U. S. S. R., Moscow
V. E. VOSKRESENSKIĬ	Université de Samara
Michel WALDSCHMIDT	Université Paris 6
Rolf WALLISSER	Universität Freiburg i. Br.
Steve WILSON	University of Durham
Jie WU	Université de Nancy I
V. I. YANCHEVSKIĬ	Acad. of Sciences B. S. S. R., Minsk

Résumés

et dates de réception des manuscrits

Conférences

KÁLMÁN GYŐRY - **Some recent applications of S-unit equations** *26.3.92*

In this survey paper, some new applications of S-unit equations are presented to certain arithmetic graphs and irreducible polynomials, to a conjecture on common polynomial divisors of trinomials, to families of solutions of decomposable form equations, to certain generalized systems of S-unit equations, and to binary forms and decomposable forms of given discriminant. Further, some consequences of a generalization of Baker's type inequalities are discussed for S-unit equations.

MARC HINDRY - **Sur les conjectures de Mordell et Lang (d'après Vojta, Faltings et Bombieri)** *4.2.92 (remarque 'dernière minute' 5.5.92)*

I present the new proof of Mordell's conjecture found by Vojta and the generalization proven by Faltings: "a subvariety of an abelian variety has only finitely many points rational over a number field, whenever it contains no translate of subabelian variety". The paper also describes further simplifications due to Bombieri and some applications of these results, especially to the study of algebraic points of given degree on a curve.

K. RAMACHANDRA - **On Riemann zeta-function and allied questions** *13.9.91 (revised 'Postscript' 25.5.92)*

A. RAPINCHUK - **Congruence subgroup problem for algebraic groups: old and new** *5.11.91*

The paper is an up-to-date survey of the congruence subgroup problem. It contains the statement of Serre's conjecture on the congruence subgroup property for S-arithmetic subgroups of simple simply connected groups of S-rank ≥ 2, and most of the results that confirm it. Besides, some new methods of attacking the congruence subgroup problem are described which provide new examples of groups with the congruence subgroup property.

A.J. SCHOLL - **Modular forms and algebraic K-theory** *14.2.92*

This paper is a slightly expanded version of the talk given at the conference. We sketch an example of a non-trivial element of K_2 of a certain threefold, whose existence is related to the vanishing of an *incomplete* L-function of a modular form at $s = 1$. This is preceded with a simple account, for the non-specialist, of some of the conjectures (mostly due to Beilinson) which relate ranks of K-groups and orders of L-functions, supplemented by examples coming from modular forms.

TETSUJI SHIODA - **Some remarks on elliptic curves over function fields** *25.11.91*

As a supplement to my talk 'Mordell-Weil lattices and sphere packings' at JA91 in Geneva, I discuss some basic results on the L-function of an elliptic curve over a function field with a finite constant field, from the viewpoint of Mordell-Weil lattices. Some explicit examples are given.

Autres exposés

YVETTE AMICE et BRUNO KAHN - **Sommes de puissances dans les corps finis** *9.1.92*

The higher levels of a field F, studied among others by Parnami, Agrawal, Rajwade and Revoy, are defined like the ordinary level, as the smallest number of n-th power summands necessary to represent -1, where n is a power of 2. When F is a finite field $\mathbb{F}_q$ (q odd), the increasing sequence of higher levels stabilises from $h(q)$ on, where $h(q)$ is the dyadic valuation of $q-1$; its supremum is denoted here by $s(q)$. It appears that $s(q) = 2$ unless $q = p$ or p^3, with $p =$char F , and $s(p^3) = 2$ or 3. If $q = p$, the Weil (or Jacobi) sums estimates imply that $s(p) = 2$ as soon as $p \geq 2^{4h(p)}$. However, computations performed up to 10^9 hint that this bound is much too big in practice, and at least for small values of $h(p)$ ($h(p) \leq 7$), one has $s(p) = 2$ as soon as $p \geq 2^{2.72h(p)}$. Similarly, computations find no prime p such that $s(p^3) = 3$ up to $p = 101\,711\,873$. We believe that these experimental results exemplify general phenomena, but so far have no theoretical explanation for them.

A-M. BERGÉ, J. MARTINET et F. SIGRIST - **Une généralisation de l'algorithme de Voronoï pour les formes quadratiques** *7.1.92*

Ainsi que Voronoï l'a montré en 1908, les formes quadratiques définies positives *parfaites* de dimension donnée peuvent être classées au moyen d'un algorithme explorant un graphe. Les résultats récents de Jaquet pour la dimension 7 indiquent clairement que cette dimension marque la limite des possibilités actuelles.

Nous montrons dans cet article comment une extension de l'algorithme original permet de traiter des variantes utiles du problème initial, et en particulier de classer les formes parfaites avec groupe d'automorphismes donné.

VALÉRIE BERTHÉ - **De nouvelles preuves "automatiques" de transcendance pour la fonction zêta de Carlitz** *25.11.91*

Carlitz a défini une fonction ζ qui est l'analogue pour le corps fini $\mathbf{F}_q$ de la fonction ζ de Riemann. Yu a montré, en utilisant les modules de Drinfeld, que $\zeta(s)/\Pi^s$ est transcendant pour tout s non divisible par $q-1$, Π étant une série formelle analogue au réel π. Je donne ici une preuve par les automates de la transcendance de $\zeta(s)/\Pi^s$ pour $q \neq 2$ et $1 \leq s \leq q-2$, en utilisant le théorème de Christol, Kamae, Mendès France et Rauzy.

GAUTAMI BHOWMIK - **Divisor functions of integer matrices: evaluations, average orders and applications** *18.11.91*

We extend the concept of divisor functions to matrices over $\mathbb{Z}$ and prove a recursion in the size of the matrix. A special case of the Köcher zeta function helps us obtain average orders.

We give examples of connections of our results with Hecke algebras and partition functions.

TED CHINBURG and BOAS EREZ - **Equivariant Euler-Poincaré characteristics and tameness** *2.12.91*

In this paper we define an Euler-Poincaré characteristic which is the basis for generalizing to tame coverings of schemes the theory of the Galois module structure of rings of algebraic integers. First we define tame G-coverings of schemes $f : X \to Y$, where G is a finite group. Then, under the assumption that the schemes are proper and of finite type over a noetherian ring A and given T a coherent G-sheaf on X, we define the Euler-Poincaré characteristic $\chi R\Gamma^+(f_*((T))$, which is an element of the Grothendieck group $CT(AG)$ of all *finitely generated* AG-modules which are *cohomologically trivial* as G-modules. In fact the definition applies to certain complexes of sheaves on X which occur in applications. In an appendix we include a proof of a variant of the well known Lemma of Abhyankar characterizing tame G-coverings of schemes.

GREGORY A. FREIMAN - **On the structure and the number of sum-free sets** *13.9.91, and in revised form 10.6.92*

A finite set A of positive integers is called sum-free if $A \cap (A+A) = \emptyset$.

For n odd, $\{1, 3, 5, ..., n\}$ and $\left\{\frac{n+1}{2}, \frac{n+3}{2}, ..., n\right\}$ are examples of such sets.

Denote by m and ℓ, respectively, the largest and smallest elements of A and by a the cardinality of A.

We show that if the cardinality of the sum-free set A does not differ much from $\frac{\ell}{2}$, then A does not differ much from one of the two examples mentioned above. More precisely, if $a > \frac{5}{12}\ell + 2$, then either all elements of A are odd or A contains both odd and even integers and $m \geq a$.

It is shown that if $a > \frac{5}{12}\ell + 2$ then the number of such sum-free sets is $O(2^{n/2})$ which proves for such sets the conjecture of P. Cameron and P. Erdös.

DAVID HARARI - **Groupes de Brauer de certaines hypersurfaces** *25.11.91*

Soit k un corps de nombres, V l'hypersurface de $\mathbf{A}^n_k$ d'équation $y^2 - az^2 = f(x_1, ..., x_{n-2})g(x_1, ..., x_{n-2})$, avec $a \in k^* - k^{*2}$, f et g polynômes irréductibles de degré 2 premiers entre eux. Soient ϕ, ψ les formes quadratiques obtenues en homogénéisant f et g ; on suppose que l'intersection de leurs noyaux est réduite à 0. Soit X un modèle projectif lisse de V. Alors, quand $n \geq 6$, X vérifie le principe de Hasse et l'approximation faible. Quand $n = 5$, l'obstruction de Brauer-Manin au principe de Hasse et à l'approximation faible pour X est la seule, et c'est encore le cas quand $n = 4$ si les coniques définies par ϕ, ψ sont lisses et se coupent transversalement suivant deux paires de points conjugués.

WERNER HÜRLIMANN - **A short proof of the Albert-Brauer-Hasse-Noether theorem** *28.10.91*

We present a short proof of the Albert-Brauer-Hasse-Noether theorem on the Brauer group of a global field. The connection between Galois cohomology and algebraic tori theory is emphasized.

Let K/k be a finite Galois extension of arbitrary fields with group G, then the relative Brauer group is $Br(K/k) \cong H^2(G, K^*) \cong H^1(G, T_1(K))$, where T_1 is the algebraic k-torus associated to the augmentation ideal I_G of G. When k is a global field, we use fundamental facts from algebraic tori theory, Tate-Nakayama duality and modern versions of Grunwald-Wang's lemma to deduce the short exact sequence

$$0 \longrightarrow Br(k) \longrightarrow \oplus Br(k_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0,$$

where k_v runs over the completions of k at all places v of k.

W. JENKNER - **Les corps p-adiques dont les groupes de Galois absolus sont isomorphes** *14.11.91*

Soit p un nombre premier quelconque (on remarquera notamment le cas $p = 2$). On considère deux extensions finies K et L de $\mathbb{Q}_p$, contenues dans une clôture algébrique $\bar{\mathbb{Q}}_p$. Si les groupes de Galois $\mathrm{Gal}(\bar{\mathbb{Q}}_p/K)$ et $\mathrm{Gal}(\bar{\mathbb{Q}}_p/L)$ sont des groupes topologiques isomorphes, on démontre que les sous-extensions abéliennes maximales de $K/\mathbb{Q}_p$ et de $L/\mathbb{Q}_p$ sont identiques.

J. KACZOROWSKI - **The boundary values of generalized Dirichlet series and a problem of Chebyshev** *24.9.91*

There is an old conjecture of Chebyshev saying that there are more primes $p \equiv 3 \pmod 4$ than $p \equiv 1 \pmod 4$. S. Knapowski and P. Turán have given a quantitative interpretation of this statement. We prove a theorem about the boudary values of general Dirichlet series and show its relevance to Chebyshev's problem. In particular it turns out that the Knapowski-Turán conjecture is false at least if we accept the Riemann Hypothesis for L-functions $\pmod 4$.

A. and J. KNOPFMACHER - **Metric properties of algorithms inducing Lüroth series expansions of Laurent series** *18.11.91*

We investigate ergodic and metric properties of the polynomial 'digits' occuring in certain Lüroth-type series representations of formal Laurent series over finite fields. In particular, relative to Haar measure on power series with zero constant term, the results stated or derived in detail include the existence almost everywhere of a Khintchine-type constant, and of various other metric conclusions on the frequency or distribution of given 'digit values'.

JOAN-C. LARIO - **Serre's conjecture on Galois representations attached to Weil curves with additive reduction** *15.11.91, and in revised form 21.4.92*

In a joint work with P. Bayer [Ba-La 91] we verify Serre's conjecture (3.2.4?) (in *Duke J.*) for the Galois representation defined by the p-torsion points of p-vertical Weil curves. In this paper our purpose is to emphasize the difference between the p-vertical and the p-horizontal cases in order to check Serre's conjecture. Several numerical examples, collected by computer calculations, lead us to give a conjecture which implies (3.2.4?) for the horizontal case.

MIROSLAV LAŠŠÁK - **Some remarks on the Pethö public key cryptosystem** *18.11.91*

This note aims to point out that under certain conditions the public key cryptosystem introduced by Pethö in [1] can be broken in polynomial time. This gives some additional conditions which should be imposed on the choice of some parameters of the secret part of this system.

TOM MEURMAN - **A simple proof of Voronoï's identity** *1.11.91*

A comparatively simple proof of Voronoï's identity is given. The proof does not depend on the functional equation for the Riemann zeta-function nor on properties of Bessel functions.

B.Z. MOROZ - **On representation of large integers by integral ternary positive definite quadratic forms** *13.9.91, and in revised form 22.10.91*

We prove a conjecture of Heath-Brown to the extent that every sufficiently large integer congruent to 7 modulo 8 is represented by the quadratic form $x^2+y^2+p^3z^2$, where p is a rational prime congruent to 5 modulo 8 (in particular, by the form $x^2+y^2+125z^2$), and discuss some related results.

RUDOLF SCHARLAU and CLAUDIA WALHORN - **Integral lattices and hyperbolic reflection groups** *20.11.91, and in revised form 21.9.92*

The aim of this paper is to study arithmetic groups of isometries of hyperbolic spaces which are generated by hyperplane reflections. This leads to the notion of reflexive Lorenzian lattices.

The main contribution of this paper is to give many new examples of such lattices in dimensions 3 and 4. These lattices give rise to maximal, pairwise non-conjugate arithmetic reflexion groups on hyperbolic 3-space, respectively 4-space. The method belongs to the arithmetic theory of quadratic forms.

HIRONORI SHIGA - **On the transcendency of the values of the modular function at algebraic points** *11.11.91, and in revised form 22.1.92*

In this note we study an abelian variety A defined over $\overline{\mathbb{Q}}$. We characterize the abelian variety of CM type by its property of periods. The obtained result yields the criterion for algebraicity of the values of the Siegel modular function at algebraic points and of various other modular functions.

S. SRINIVASAN - **Two results in number theory** *13.12.91, and in revised form 11.6.92*
Here we present two results which were observed while studying a conjecture from S.K. Zaremba.

V.I. YANCHEVSKIĬ - **K-unirationality of conic bundles over large arithmetic fields** *15.11.91*

We prove that if a conic bundle surface over a rational curve is defined over a pseudo-real closed (or p-adically closed) field K and has a K-rational point then it is K-unirational. We also obtain the corresponding result for the so-called 'large' arithmetic fields K, which are suitable intersections of finitely many Henselizations of $\mathbb{Q}$.