**Department of Mathematics**
**University of Stellenbosch**

Van der Sterr Building
7602 Stellenbosch

*Prof. B.W. Green*

e-mail: bwg@sun.ac.za
Tel: (021) 808-3284

21 February 2005

# Report on the International Workshop on

# "Arithmetic Geometry, Related Areas and Applications"

# University of Stellenbosch, 1 – 4 February 2005

**VENUE: The Department of Mathematics, University of Stellenbosch**

**AIM:** This workshop was the sixth meeting of its kind, which has been organized at the University of Stellenbosch over the past eight years. Originally these workshops were held as part of a *Volkswagen Foundation Partnership Project* on *Arithmetic Geometry and Data Security* between the University of Essen and the University of Stellenbosch with participation by other local universities. Following this project, which ended in 2001, the local group at Stellenbosch has continued to grow, with new appointments and a number of Masters and PhD students. The workshops have continued to be held biannually as one of the research stimulating activities of our group.

The present meeting was organized as a research conference in arithmetic geometry and its applications. The topics of the talks all fell within this broad area (see the enclosed programme) and included both research and survey talks. One afternoon was set aside for talks by graduate students, who reported on the research progress towards the projects they are working on.

**AIMS Symposium Day:** One special activity held during the workshop was an AIMS Symposium Day with special survey lectures. This was held at the *African Institute for the Mathematical Sciences (AIMS)* in Muizenberg and was organized jointly with *Prof Fritz Hahne,* the Director of AIMS. The event was attended by the participants of the workshop as well as the fourty four AIMS students, who are selected from all over Africa and follow a one year post graduate diploma in the mathematical sciences. This event was very successful, introducing the AIMS students to selected topics from arithmetic geometry, data security and computuational algebra. It also provided the opportunity for the visiting academics to become familiar with the AIMS project and the success it has been. For information concerning AIMS we refer to http://www.aims.ac.za

The meeting was supported by the the newly formed *University of Stellenbosch, Center for Experimental Mathematics,* the *Rubbi Fund of the Mathematics Department,* the *African Institute for the Mathematical Sciences* as well personal research grants. The organizers are grateful for this support and also to all the visiting experts, for helping to make this a successful meeting.

*Prof. Barry Green*

**ATTACHMENTS:**

i) List of Participants

ii) Programme

iii) Abstracts

## Participants

Ilhem Benzaoui (Stellenbosch)
benzaoui@sun.ac.za

Florian Breuer (Stellenbosch)
fbreuer@sun.ac.za

Louis Brewis (Stellenbosch)
13448900@sun.ac.za

Sinnou David (Paris)
david@math.jussieu.fr

Gerhard Frey (Essen)
frey@exp-math.uni-essen.de

Ernst Gekeler (Saarbrucken)
gekeler@math.uni-sb.de

Martine Girard (Sydney)
girard@maths.usyd.edu.au

Barry Green (Stellenbosch)
bwg@sun.ac.za

Yuki Haraguchi (Tokyo)
haraguti@grad.math.chuo-u.ac.jp

Marc Hindry (Paris)
hindry@math.jussieu.fr

Kenneth Hughes (Cape Town)
hughes@maths.uct.ac.za

Paul Joubert (Stellenbosch)
13266616@sun.ac.za

Arnold Keet (Stellenbosch)
keetap@sun.ac.za

David Kohel (Sydney)
kohel@maths.usyd.edu.au

Marelize Kriel (Stellenbosch)
secretjude@mweb.co.za

Boris Kunyavski (Tel Aviv)
kunyav@macs.biu.ac.il

Archie Karumbidze (Stellenbosch)
archiek@sun.ac.za

Ernest Lötter (Stellenbosch)
ecl@sun.ac.za

Yasuhiro Niitsuma (Tokyo)
niitsuma@grad.math.chuo-u.ac.jp

Rafi Omar (Western Cape)
romar@uwc.ac.za

Amilcar Pacheco (Rio de Janeiro)
amilcar@impa.br

Helmut Prodinger (Stellenbosch)
hproding@sun.ac.za

Georg Rück (Kassel)
rueck@mathematik.uni-kassel.de

Tsutomu Sekiguchi (Tokyo)
sekiguti@math.chuo-u.ac.jp

Noriyuki Suwa (Tokyo)
suwa@math.chuo-u.ac.jp

Christine Swart (Cape Town)
cswart@maths.uct.ac.za

Brink van der Merwe (Stellenbosch)
abvdm@sun.ac.za

Koos van Zyl (Pretoria)
koos@up.ac.za

Lesley Wessels (Stellenbosch)
lwessels@sun.ac.za

# Workshop on Arithmetic Geometry

# Related Areas and Applications

# Programme

# University of Stellenbosch, 1 – 4 February 2005

**Venue:** *Department of Mathematics, Van der Sterr Building, 3021*

**Organizers:** Florian Breuer, Barry Green (Stellenbosch University)

**Tuesday 1 February**

9:00 - 10:00 *M. Hindry*, On the number of primes represented by polynomials

10:00 - 10:30 *Tea*

10:30 - 11:30 *T. Sekiguchi*, Geometric aspects on the addition algorithm on the Jacobian variety of a $C_{ab}$ curve

11:30 - 14:30 *Admin and Lunch*

14.30 - 15.20 *H.-G. Rück*, Curves over finite fields with the maximal number of rational points

15:40 - 16.30 *D. Kohel*, Constructing CM invariants of genus 2 curves

16:40 - 17:30 *E.-U. Gekeler*, Frobenius distributions of elliptic curves

**Wednesday 2 February:** Symposium day at the *African Institute for the Mathematical Sciences*

9:00 - 10:00 *G. Frey*, Applications of Arithmetic Geometry to Data Security

10:30 - 11:20 *D. Kohel*, Introduction to Magma and Applications

11:40 - 12:30 *E.-U. Gekeler*, Heuristics in Number Theory

12.30 - 14.00 *Lunch*

14.30 - 17:30 *Outing*

**Thursday 3 February**

9:00 - 10:00 *N. Suwa*, Twisted Kummer and Kummer-Artin-Schreier Theories

10:00 - 10:30 *Tea*

10:30 - 11:20 *B. Kunyavski*, Application of arithmetic geometry to the characterization of finite solvable groups

11:30 - 12:20 *M. Girard*, Maximality of the Weierstrass subgroup of the generic genus $g$ curve

12:30 - 14:30 *Lunch*

14.30 - 15.20 *Y. Haraguchi*, On non-commutative extensions of $\mathbb{G}_a$ by $\mathbb{G}_m$ over an $\mathbb{F}_p$-algebra

15:40 - 16.30 *Y. Niitsuma*, On the extensions of $\widehat{W}_n$ by $\widehat{\mathcal{G}}^{(\mu)}$ over a $\mathbb{Z}_{(p)}$-algebra

16:40 - 17:30 *M. Kriel*, Endomorphism rings of hyperelliptic Jacobians

**Friday 4 February**

9:30 - 10:30 *A. Pacheco*, Rank of abelian varieties over function fields

10:30 - 11:00 *Tea*

11:00 - 12:00 *S. David*, Uniformity questions in the Mordell-Lang problem

12:00 - 14:30 *Lunch*

14.30 - 15.20 *F. Breuer*, Galois representations associated to Drinfeld modules

15:40 - 16.30 *K. Hughes*, Wolstenholme's Theorem, Formal groups, and $p$-adic $L$-functions

16:40 - 17:30 *C Swart*, A very simple attack on an elliptic curve $E/\mathbb{F}_p$ where $\#E(\mathbb{F}_p) = p - 1$ or $p$.

**Enquiries:**

*Florian Breuer* **Tel:** (021) 808 3288 **e-mail:** fbreuer@sun.ac.za

*Barry Green* **Tel:** (021) 808 3284 **e-mail:** bwg@sun.ac.za

## Abstracts Submitted

**Speaker:** Florian Breuer, Department of Mathematics, University of Stellenbosch.

**Title:** *Galois representations associated to Drinfeld modules.*

**Abstract:** I will report on joint work with Richard Pink, where we prove that the image of the Adelic Galois representation attached to a Drinfeld $A$-module of generic characteristic is open if the Drinfeld module in question is defined over a finitely generated - but not finite - extension of the quotient field of $A$. This result is derived from similar results concerning the adelic openness of etale and analytic monodromy representations. These results are in turn proved using known results on $p$-adic Galois representations and strong approximation.

**Speaker:** Sinnou David, Univ. de Paris VI, Paris.

**Title:** *Uniformity questions in the Mordell-Lang problem.*

**Abstract:** Let $C$ be a curve of genus at least 2 defined over a number field $K$. It is known that the set of $K$-rationnal points of $C$ is finite (Faltings), it is also known that the set of torsion points (over the algebraic closure of $K$) of the jacobian $J$ of $C$ that belong to $C$ is finite (Raynaud). It is conjectured that the number of such points are bounded in some uniform way in terms of the genus of $C$ and the rank of the Mordell-Weil group of $C$. We address such questions when $J$ is isogenous to a power of an elliptic curve.

**Speaker:** Gerhard Frey, Institute for Experimental Mathematics, University of Duisburg-Essen.

**Title:** *Applications of Arithmetic Geometry to Data Security.*

**Abstract:** Arithmetic Geometry is one of the most important areas of recent mathematical research. It combines methods from algebraic and analytic number theory with algebraic geometry and topology. A key ingredient is the study of the arithmetic of Galois representations. The most spectacular results obtained are Faltings' proof of Mordell's conjecture and Wiles' proof of Fermat's Last Theorem.

In the lecture we explained how the same methods can be used for the design of public key cryptosystems based on the Discrete Logarithm problem in the group of rational points of algebraic groups over finite fields, e.g. in the group of rational points of elliptic curves over finite fields. It turns out that these applications have constructive aspects (e.g. point counting by computing étale and crystalline cohomology groups) as well as destructive aspects (use of Tate duality to transfer the Discrete Logarithm into Brauer groups, attacks using scalar restriction) and that they lead to new interesting questions in computational number theory, for instance about Brauer groups of local and global fields.

**Speaker:** Ernst-Ulrich Gekeler, Fachrichtung 6.1 Mathematik, Universität des Saarlandes.

**Title:** *Frobenius distributions of elliptic curves.*

**Abstract:** Let $E/\mathbb{F}_q$ be an elliptic curve over the finite field $\mathbb{F}_q$ with $q$ elements. For each prime $l$ different from the characteristic $p$ of $\mathbb{F}_q$, its Frobenius element $F = F(E/\mathbb{F}_q)$ is a well defined conjugacy class in $\mathrm{GL}(2, \mathbb{Z}_l)$. Motivated from e.g. the Cebotarev density theorem and various proved or conjectured assertions involving the $F(E/\mathbb{F}_q)$, we propose a rather general equidistribution hypothesis (H) if $E$ varies in a family. Although we have no idea how to prove (H), it leads to several conclusions which make sense independently of the truth of (H). For instance, (H) implies

- an asymptotic description for $x \to \infty$ of the counting function

$$H(t,x) = \#(E/\mathbb{F}_p \text{ with Frobenius trace } t)$$

( $t$ a fixed integer) and $p \leq x$;

- a similar description of the number of $E/\mathbb{F}_p$, where the $l$-part of $E(\mathbb{F}_p)$ is a fixed abelian $l$-group.

The first one is proved in Int. Math. Res. Notes 37, 1999-2018, 2003, the proof of the second one is presently being written up.

**Speaker:** Ernst-Ulrich Gekeler, Fachrichtung 6.1 Mathematik, Universität des Saarlandes.

**Title:** *Heuristics in Number Theory.*

**Abstract:** In number theory, as in other mathematical disciplines, we often meet the following situation: A certain quantity is restricted through proved or conjectural properties that ought to hold, and seems to behave "randomly" for the rest. Considering that quantity as a random variable, we can try to describe it through a stochastic model. This often leads to reasonable conjectures or even theorems, despite the purely heuristic (and mathematically inexact) way how we were led to the conclusion.

This is illustrated with the following cases, partially well-known and classical, partially rather new:

- distribution of prime numbers in arithmetic progressions (Dirichlet's theorem).
- local behaviour of Galois extensions of number fields (Cebotarev's theorem).
- statistics of finite abelian groups.
- statistics of class groups of number fields (Cohen-Lenstra philosophy).
- statistics of elliptic curves over finite fields.

**Speaker:** Martine Girard, Department of Mathematics, University of Sydney.

**Title:** *Maximality of the Weierstrass subgroup of the generic genus $g$ curve.*

**Abstract:** The group generated by the Weierstrass points of a curve in its Jacobian, the Weierstrass subgroup, is a geometric invariant of the curve. We show that the Weierstrass subgroup of the generic curve of genus $g \geq 3$ is a free abelian group of rank $g(g^2-1)-1$. This is joint work with David Kohel and Christophe Ritzenthaler.

**Speaker:** Yuki Haraguchi, Department of Mathematics, Chuo University.

**Title:** *On non-commutative extensions of $\mathbb{G}_a$ by $\mathbb{G}_m$ over an $\mathbb{F}_p$-algebra.*

**Abstract:** Let $A$ be a commutative ring, and let $G$, $H$ be algebraic groups or formal groups over $A$. It is an important problem to determine $\mathrm{Ext}^1_A(G,H)$, especially in elementary cases. The results were arranged, for example, in ⟨ Groupes algébriques et corps de classes ⟩ by Serre or ⟨ Groupes algébriques ⟩ by Demazure and Gabriel, in case where $A$ is a field.

In this talk, we mention an explicit description of the non-commutative extensions of $\mathbb{G}_{a,A}$ (resp. $\widehat{\mathbb{G}}_{a,A}$) by $\mathbb{G}_{m,A}$ (resp. $\widehat{\mathbb{G}}_{m,A}$) over an $\mathbb{F}_p$-algebra $A$, developing the method of Sekiguchi and Suwa to determine commutative extensions of $\mathbb{G}_{a,A}$ (resp. $\widehat{\mathbb{G}}_{a,A}$) by $\mathbb{G}_{m,A}$ (resp. $\widehat{\mathbb{G}}_{m,A}$).

**Speaker:** Marc Hindry, Université Denis Diderot, Paris.

**Title:** *On the number of primes represented by polynomials.*

**Abstract:** We present a joint work with Tanguy Rivoal proposing a new approach towards the so-called Bateman-Horn conjecture which is a quantitative version of a conjecture of Schinzel. This describes the asymptotic behaviour of the number of integral values less than a given $X$ where $r$ polynomials (satisfying suitable conditions) take simultaneously prime values. We in fact reduce the conjecture to the hypothesis that one may exchange a limit and an infinite summation for some explicit

coefficients. Unfortunately the justification of this exchange must be left unanswered for the moment except in the case of one linear polynomial, corresponding to Dirichlet's theorem.

**Speaker:** Marelize Kriel, Department of Mathematics, University of Stellenbosch.

**Title:** *Endomorphism rings of hyperelliptic Jacobians.*

**Abstract:** In this talk I intend to show how facts about $\mathbb{Z}$-orders in semisimple algebras can be transformed into facts about abelian varieties and how these might be used to determine the isomorphism type of the endomorphism ring of a Jacobian variety of a hyperelliptic curve.

I will also discuss how to construct modular equations for hyperelliptic curves and how their factorization patterns give us more information on the $\ell$-isogenous abelian varieties in the isogeny class of the Jacobian. Finally, I will illustrate how in certain special cases this information is enough to completely determine the endomorphism ring of a hyperelliptic Jacobian up to isomorphism.

**Speaker:** Boris Kunyavski, Department of Mathematics, Bar-Ilan University.

**Title:** *Application of arithmetic geometry to the characterization of finite solvable groups*

**Abstract:** We present an explicit family of identities in two variables defining the class of finite solvable groups (as the Engel identities characterize finite nilpotent groups). The proof is not purely group-theoretic but involves quite a lot of computations with algebraic varieties over finite fields: Hasse-Weil estimates for singular curves, Deligne's conjecture (proved by Zink-Pink-Fujiwara), estimates of l-adic Betti numbers (Adolphson-Sperber and N.Katz), etc.

This is a joint work with T. Bandman, G.-M. Greuel, F. Grunewald, G. Pfister, and E. Plotkin.

**Speaker:** Yasuhiro Niitsuma, Department of Mathematics, Chuo University.

**Title:** *On the $\widehat{W}_n$ by $\widehat{\mathcal{G}}^{(\mu)}$ over a $\mathbb{Z}_{(p)}$-algebra.*

**Abstract:** Let $A$ be a commutative ring, and let $G$ and $H$ be algebraic groups or formal groups over $A$. It is an interesting problem to determine $\mathrm{Ext}^1_A(G,H)$ or $H^2_0(G,H)$, which is now solved completely when $A$ is a field. There are related works by Weisfeiler, Waterhouse, Kunyavski and so on in case where $A$ is not a field. Furthermore $H^2_0(G,H)$ is determined explicitly in a series of works by Sekiguchi and Suwa when $G = W_n$ or $\mathcal{G}^{(\lambda)}$, $H = \mathbb{G}_m$ or $\mathcal{G}^{(\mu)}$ and $A$ is a $\mathbb{Z}_{(p)}$-algebra. Here $\mathcal{G}^{(\mu)}$ is a group scheme which gives a deformation between $\mathbb{G}_a$ and $\mathbb{G}_m$.

In this talk, we will give an explicit description of $H^2_0(\widehat{W}_{n,A}, \widehat{\mathcal{G}}^{(\mu)}_A)$ when $A$ is a $\mathbb{Z}_{(p)}$-algebra, generalizing the result for $H^2_0(\widehat{W}_{n,A}, \widehat{\mathbb{G}}_{m,A})$ by Sekiguchi and Suwa. It is crucial to combine two exact sequences

$$0 \to \widehat{\mathcal{G}}^{(M)} \to \prod_{B/A} \widehat{\mathbb{G}_{m,B}} \to \widehat{\mathbb{G}}_{m,A} \to 0$$

and

$$0 \to W^{(M)} \to \prod_{B/A} W_B \to W_A \to 0$$

where $A = \mathbb{Z}_{(p)}[M]$-algebra and $B = A[t]/(t^2 - Mt)$

**Speaker:** Amilar Pacheco, Universidade Federal do Rio de Janeiro.

**Title:** *Rank of abelian varieties over function fields.*

**Abstract:** Let $C$ be a smooth projective irreducible curve defined over a number field $k$, $K = k(C)$ its function field, $A/K$ an abelian variety over $K$ and $B$ its $K/k$-trace. For any $k$-Galois cover $C'/C$ we obtain the variation of the rank of $A(K')/B(k)$, where $K'$ denotes the function field $k(C')$ of $C'$, vis-a-vis Ogg's geometric bound. We give examples of towers of function fields where the rank decreases slower than the heuristics would predict.

**Speaker:** Hans-Georg Rück, Fachbereich für Mathematik und Informatik Universität Kassel.

**Title:** *Curves over finite fields with the maximal number of rational points.*

**Abstract:** For applications in coding theory one is interested in curves over finite fields with many rational points. The number of rational points on a curve of genus $g$ over a finite field with $q$ elements is bounded by the Weil bound $1+q+2g\sqrt{q}$. Curves, where this bound is attained, are called maximal curves. We give necessary and suffient conditions for curves to be maximal. In particular we discuss abelian extensions of maximal curves.

**Speaker:** Tsutomu Sekiguchi, Department of Mathematics, Chuo University.

**Title:** *Geometric aspects on the addition algorithm on the Jacobian variety of a $C_{ab}$ curve.*

**Abstract:** In this talk we discuss the addition computation on Jacobian varieties of curves using its singular plane model. Given a nonsingular curve C, let $C_1$ be its singular (especially plane) $C_A$ model. After discussing the relationship between the generalized Jacobian variety of $C_1$ and the Jacobian variety of $C$, we show that Arita's algorithm for non singular $C_A$ curves also works for generalized Jacobian variety of singular $C_A$ curve $C_1$. This means that we can compute addition on Jacobian variety of any curve (with at least one rational point) using its singular $C_A$ models.

**Speaker:** Noriyuki Suwa, Department of Mathematics, Chuo University.

**Title:** *Twisted Kummer and Kummer-Artin-Schreier theories.*

**Abstract:** The inverse Galois problem asks if, given a field $k$ and a finite group $G$, there exists a Galois extension $K$ of $k$ with $\mathrm{Gal}(K/k) = G$. The theory of generic polynomials is one approach to the problem, constructing explicitly a polynomial which defines a Galois covering with group $G$ over a rational variety over $k$ and parametrizes the Galois extensions $K$ over $k$ with $\mathrm{Gal}(K/k) = G$. Recently, it was observed by Rikuna and Komatsu that Cebysev polynomials can be regarded as a generic polynomial for cyclic extensions over the maximal real subfiled of a cyclotomic field. In this talk, we give an formulation of their results in the frame of group scheme theory and mention some examples of cohomology groups concerning related group schemes.

**Speaker:** Christine Swart, Department of Mathematics, University of Cape Town.

**Title:** *A very simple attack on an elliptic curve $E/\mathbb{F}_p$ where $\#E(\mathbb{F}_p) = p - 1$ or $p$.*

**Abstract:** We use the division polynomials of an elliptic curve and an old result on elliptic divisibility sequences to construct a particularly simple attack on the elliptic curve discrete logarithm problem in the MOV and anomalous cases.