ABELIAN VARIETIES AND RELATIONS TO NUMBER THEORY, GEOMETRY AND PHYSICS

SCHLOSS RINGBERG

JULY 24-30, 1988

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26

D - 5300 Bonn 3

MPI/88-56

Diese Tagung wurde finanziert aus Mitteln der Deutschen Forschungsgemeinschaft sowie der Max-Planck-Gesellschaft. Wir danken diesen beiden Institutionen herzlich für die Bereitstellung der Mittel.

G. Wüstholz
D. Zagier

Contents

List of Participants

E. Bayer	(Geneva)
J.-B. Bost	(Paris)
W.D. Brownawell	(Pennsylvania)
E. Date	(Kyoto)
B. Edixhoven	(Utrecht)
G. van der Geer	(Amsterdam)
T. Ibukiyama	(Fukuoka)
T. Katsura	(Yokohama)
J. Kramer	(Zurich)
H. Lenstra	(Berkeley)
D.W. Masser	(Ann Arbor)
Y. Namikawa	(Bonn)
T. Oda	(Hokkaido)
J. Oesterlé	(Paris)
F. Oort	(Utrecht)
N. Schappacher	(Bonn)
R. Schoof	(Pisa)
J.-P. Serre	(Paris)
A. Silverberg	(Ohio)
Ch. Soulé	(Paris)
G. Wüstholz	(Zurich)
J.-P. Wintenberger	(Paris)
D. Zagier	(Bonn)

Program of the Conference on 'Abelian Varieties and Relations to Number Theory, Geometry and Physics'

Part I.

Monday, July 25th

10.00 - 11.00	J.-P. Serre: Abelian varieties and their division points I
11.15 - 12.15	G. van der Geer: The Schottky Problem
16.00 - 17.00	J.-B. Bost: Quillen metrics on Riemann surfaces
17.15 - 18.15	F. Oort: Supersingular abelian varieties

Tuesday, July 26th

09.30 - 10.30	G. Wüstholz: Transcendence applied to isogenies
11.00 - 12.00	E. Date: Solvable lattice models and affine Lie algebras
12.00 - 12.15	Program discussion II
Afternoon	Walk to *Wallberg*

Program of the Conference on 'Abelian Varieties and Relations to Number Theory, Geometry and Physics'

Part II.

Wednesday, July 27th

09.30 - 10.30 J.-P. Serre:
Abelian varieties and their division points II

11.00 - 12.00 B. Edixhoven:
Hecke action on the component groups of the Néron model of the Jacobian of a modular curve

16.00 - 17.00 H. Lenstra:
Primality testing

17.15 - 18.15 J.-P. Wintenberger:
p-adic Hodge theory for families of abelian varieties

21.00 **Concert**

Gülsin Onay-Schappacher

F. Chopin Sonate en si mineur
C. Franck Prélude, Chorale et Fugue
A. Saygun Sonatine

Thursday, July 28th

09.00 - 09.50 T. Ibukiyama:
Supersingular abelian surfaces and automorphism groups of lattices

10.00 - 10.50	T. Katsura: Quotients of abelian surfaces in characteristic p
11.00 - 11.50	A. Silverberg: Fiber systems of polarized abelian varieties
13.00	Beginning of the sightseeing tour to *Kloster Ettal* and *Schloss Linderhof*

Program of the Conference on 'Abelian Varieties and Relations to Number Theory, Geometry and Physics'

Part III.

Friday, July 29th

09.30 - 10.30	D.W. Masser: Isogenies of elliptic curves
11.00 - 12.00	N. Schappacher: Kolyvagin's proof of the finiteness of $E(\mathbb{Q})$ and the Tate-Shafarevich group for certain $E/\mathbb{Q}$
16.00 - 17.00	Ch. Soulé: Another proof of Mordell's conjecture over function fields (d'après P. Vojta)
17.15 - 18.15	J.-P. Serre: Abelian varieties and their division points III

Title: *Green functions, regularized determinants on curves, and theta functions*

Author: *Jean-Benoît BOST*

Address: *ENS, 45 rue d'Ulm, 75005 Paris, France*

Let X be a compact connected Riemann surface, of genus $g \geq 1$. Using the Arakelov - Green function G of X and the theta function of the jacobian of X, Faltings defines metrics on the determinant of the cohomology of line bundles over X, and a new invariant $\delta(X)$ ($\in \mathbb{R}$) of X ([F]). We discuss some relations between G, the theta function, $\delta(X)$, the Faltings metrics and the regularized determinant of the Laplace operator. These extend classical formulae on elliptic functions (recovered when $g=1$).

Theorem 1 ([B]). *There exists* $A(X)$ *such that for any* $(x,y) \in X^2$, $x \neq y$

$$\log G(x,y) = \frac{1}{g!} \int_{\Theta+x-y} \log \|\vartheta\| \, \mu^{g-1} + A(X) .$$

In this formula, Θ is the theta divisor in $\mathrm{Pic}_{g-1}(X)$, $\|\vartheta\|$ is the function $\mathrm{Pic}_{g-1}(X) \to \mathbb{R}_+$ defined in [F], and μ the translation invariant $(1,1)$ form on $\mathrm{Pic}_{g-1}(X)$ Poincaré dual to Θ.

Theorem 2 ([B]). *Suppose* $g = 2$ *and denote*

$$\mathcal{P} = \{\text{even theta characteristics}\} \subset \mathrm{Pic}_1(X)$$

$$\|\Delta_2\| = 2^{-12} \prod_{M \in \mathcal{P}} \|\vartheta\|^2 (M)$$

$$\|H\| = \exp \left[\frac{1}{2} \int_{\mathrm{Pic}_1(X)} \log \|\vartheta\| \mu^2\right].$$

Then $\quad \delta(X) = - 16 \log (2\pi) - \log \|\Delta_2\| - 4 \log \|H\|.$

If ξ is a holomorphic vector bundle on X, and if ξ and ω_X are equipped with $\mathcal{C}^\infty$ hermitian metrics $\|\cdot\|_\xi$ and $\|\cdot\|_{\omega_X}$, we define the Quillen metric on $\det R\Gamma(X;\xi)$ as in [D], §1.2. When ω_X is equipped with the Arakelov metric $\|\cdot\|_A$ (cf.[F]) and $\xi = \mathcal{O}$ is equipped with the trivial metric $\|\cdot\|_0$ ($\|1\|_0 = 1$), we denote, using the notations of [D],§1.2:

$$\det{}'(\bar{\partial}^*\bar{\partial})_A = \det{}'\bar{\partial}^*\bar{\partial};$$
$$A(X) = \langle 1,1 \rangle_{\mathcal{C}^\infty(X)} .$$

Theorem 3 (compare [D] - [ABNMV]). *Let* ξ *be a line bundle on* X, *and* $\|\cdot\|_\xi$ *a smooth admissible metric on* ξ (cf.[F], §3). *Denote* $\|\cdot\|_F$ *the Faltings metric on* det $R\Gamma(X;\xi)$ *associated to* $\|\cdot\|_\xi$ (cf.[F], th.1 and p.401), *and denote* $\|\cdot\|_Q$ *the Quillen metric on* det $R\Gamma(X;\xi)$ *defined using the metric* $\|\cdot\|_A$ *on* ω_X *and the metric* $\|\cdot\|_\xi$ *on* ξ. *We have:*

$$\|\cdot\|_Q = \left[\frac{\pi^g \det'(\bar{\partial}^*\bar{\partial})_A}{A(X)}\right]^{-\frac{1}{2}} \|\cdot\|_F$$

Theorem 4 .

$$\delta(X) = -6 \log \left[\frac{\det'(\bar{\partial}^*\bar{\partial})_A}{A(X)}\right] + (2-2g)\, M - 2g \log \frac{\pi}{4} \text{ , } \textit{where}$$

$$M = 24\, \zeta'(-1) - 3 + 4 \log 2.$$

This result is closely related to a conjecture of Gillet and Soulé. Its proof uses a joint work with J.M. Bismut, where we study the Quillen metric for degenerating families of complex curves.

References:

[ABMNV] L. Alvarez-Gaumé, J.-B. Bost, G. Moore, P. Nelson, C. Viefa: Bosonization in arbitrary genus. Comm. Math. Phys. 112(1987) 503-552

[B] J.-B. Bost: Fonctions de Green, fonctions thêta et courbes de genre 2. CRAS - Paris 1987

[D] P. Deligne: Le déterminant de la cohomologie. Contemporary Math. 67(1987) 93-178

[F] G. Faltings: Calculus on arithmetic surfaces. Ann. Math. 118(1984) 387-424

Title: *Solvable lattice models and affine Lie algebras*

Author: *Etsuro DATE*

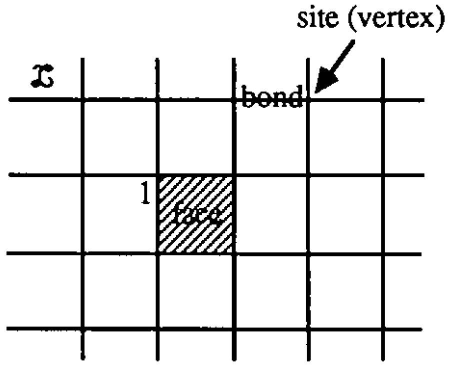
Address: *Dept. Math., College of General Education, Kyoto University,*
Kyoto, 606 Japan

This talk is based on our work at Kyoto with M. Jimbo, A. Kuniba, T. Miwa and M. Okado. We are studying solvable lattice models in 2-dimensions, and are interested in their connection with the representation theory of affine Lie algebras. We calculate local state probabilities of solvable lattice models by employing Baxter's corner transfer matrix method. In the course we encounter the quantity which we call 1-dimensional (1D) configuration sum. One of our results is that these 1D configuration sums are identified with the string functions or the branching coefficients in the representation theory of affine Lie algebras. The latter are known to be modular forms (of one variable). Thus we have the modular property related to affine Lie algebras in the theory of solvable lattice models.

A *2-dimensional lattice statistical model* on a 2-dimensional square lattice $\mathfrak{L}$ is defined by giving the following data

(i) Fluctuation variable σ on each bond and/or site with values in some set $\mathcal{A}$ (these are called *local states*).

(ii) *Boltzmann weight* for each configuration of local states around a vertex $\alpha \overset{\mu}{\underset{\beta}{+}} \nu \leftrightarrow$ $W(\alpha\beta\mu\nu)$ (*vertex model*), or around a face ${}^{a}_{d}\square^{b}_{c} \leftrightarrow W(abcd)$ (*face model*), or a mixture of these.



With these data we have a statistical model on the lattice $\mathfrak{L}$. Boltzmann weights describe interactions of local states (here we are considering the simple cases of interactions).

One of the goals of the statistical mechanics is to calculate macroscopic quantities (like the probabilities of the occurance of specified configurations) from the knowledge of the microscopic quantities (like Boltzmann weights) in the limit $|\mathcal{L}| \to \infty$ (the thermodynamic limit). One of such is the *local state probability (LSP)* (for face models) (or 1-point function) $P(a) = \mathrm{Prob}\ (\sigma_1 = a)$, that is, the probability of finding configurations such that the local state at a specified site 1 takes a given state a. By Boltzmann's principle, this may be evaluated as

$$P(a) = \lim_{|\mathcal{L}| \to \infty} \frac{1}{Z} \sum_{\text{configurations}} \delta(\sigma_1 = a) \prod_{\text{faces}} W(\sigma_i \sigma_j \sigma_k \sigma_l), \qquad {}^{i}_{l}\square^{j}_{k}$$

where $Z = \sum_{\text{configurations}} \prod_{\text{faces}} W(\sigma_i \sigma_j \sigma_k \sigma_l)$ is the *partition function*. While taking the limit we fix the local states on boundaries of $\mathcal{L}$ to be in a *ground state*. This is a configuration of local states that contributes to the partition function Z most.

For general (arbitrary) Boltzmann weights this calculation is very difficult to get limit. Therefore the first task is to single out a nice class of lattice models for which we can, at least, calculate Z or P(a). Through the works of Onsager, Baxter and others, the importance of the *Yang-Baxter equation (YBE)* (or the *Star-Triangle relation (STR)* depending on the context) in this context has been recognized. The YBE (for the vertex case) for linear operators $W_{VV'}$ etc. is the condition of the commutativity of the following diagram:

$$\begin{tikzcd}
 & V \otimes V' \otimes V'' \arrow[dl, "W_{VV'}(u) \otimes 1"'] \arrow[dr, "1 \otimes W_{V'V''}(v)"] & \\
V' \otimes V \otimes V'' \arrow[d, "1 \otimes W_{VV''}(u+v)"'] & & V \otimes V'' \otimes V' \arrow[d, "W_{VV''}(u+v) \otimes 1"] \\
V' \otimes V'' \otimes V \arrow[dr, "W_{V'V''}(v) \otimes 1"'] & \circlearrowright & V'' \otimes V \otimes V' \arrow[dl, "1 \otimes W_{VV'}(u)"] \\
 & V'' \otimes V' \otimes V &
\end{tikzcd}$$

Here V, V', V'' are vector spaces. Matrix elements of these $W_{VV'}$, etc. give us Boltzmann weights. Here we allow that the operators $W_{VV'}$, etc. depend on an extra parameter $u \in \mathbb{C}$ (spectral parameter). In other words, we consider 1-parameter family of lattice models. We call the models defined through solutions of the YBE (STR) *solvable models.*

There are several known solutions of the YBE. Here we take solutions related to affine Lie algebras $A_n^{(1)}$, $B_n^{(1)}$, $C_n^{(1)}$, $D_n^{(1)}$ found by Bazhanov, Jimbo and others. For simplicity, we consider the case $A_n^{(1)}$ in the following. From this solution we construct a *vertex model* whose local state takes values in the set of the *weights of the vector representation* of $s\ell(n+1,\mathbb{C})$, $\Theta_{n,1} = \{\eta_0,\ldots,\eta_n\}$, $\eta_i = \varepsilon_i - \frac{1}{n+1}\sum_{j=0}^{n} \varepsilon_j$ $(\varepsilon_0,\ldots,\varepsilon_n$ ONS) and whose Boltzmann weights are given by the matrix elements of the solution of the YBE of this case. Boltzmann weights depend on two parameters w,x (w being a multiplicative spectral parameter). This model can be also formulated as a face model whose set of local states consists of *level 1 weights of the affine Lie algebra* $A_n^{(1)}$. As for the explicit form of the Boltzmann weights of this model we refer to [1].

We calculate the LSPs of this face model. For this purpose we apply Baxter's *corner transfer matrix method* (for which we refer to Baxter's book "Exactly solved models in statistical mechanics" Academic 1982). This reduces the calculation of the LSPs which are in its original form a sum over 2-dimensional configurations (on a 2-dimensional lattice) to 1D configuration sums. This is a great simplification. Let us consider in the parameter region $x \approx 0$, $|w|<1$. As a result of the application of the corner transfer matrix method we are lead to the *1D configuration sum* of the form

$$f_m(\gamma,\eta;q) = \Sigma\, q^{\Sigma_{j=1}^{m} jH(\eta^{(j)},\eta^{(j+1)})},$$

where $\gamma \in$ the weight lattice of $s\ell(n+1,\mathbb{C})$, $\eta^{(m+1)} = \eta$, and $\eta^{(1)},\ldots,\eta^{(m)}$ run over $\Theta_{n,1}$ with the condition $\eta^{(1)}+\ldots+\eta^{(m)} = \gamma$. The function H is given by $H(\eta_\mu,\eta_\nu) = 0$ if $\mu < \nu$, 1 if $\mu \geq \nu$, where $\eta_\mu,\eta_\nu \in \Theta_{n,1}$. In this parameter region $x \approx 0$, $|w|<1$, ground states are constant on the NS-SW direction, and are labeled by the fundamental weights Λ_i of $A_n^{(1)}$. Thus they are given by 1-dimensional sequences of weights of level 1 $p_\Lambda = (p_\Lambda^{(j)})$, $(p_\Lambda^{(j)}) = \Lambda_{\overline{\mu+j-1}}$, $\Lambda = \Lambda_\mu$ and $\bar{m}$ signifies m (mod.n+1).

This 1D configuration relates to the string function of $A_n^{(1)}$ in the following way. By *path* $p = (p^{(j)})$, $j \geq 1$ we mean a sequence of local states such that $\eta^{(j)}(p) = p^{(j+1)} - p^{(j)} \in \Theta_{n,1} = \{\eta_0,\ldots,\eta_n\}$. Let Λ be a fundamental weight. We set

$$P(\Lambda) = \bigcup_{m=0}^{\infty} P^{(m)}(\Lambda), \quad P^{(m)}(\Lambda) = \{\, p \mid p^{(j)} = p_\Lambda^{(j)} \ \ j \geq m+1 \}$$

and define the *degree* of a path p by

$$\omega(p) = \sum_{j=1}^{\infty} j\,(H(\eta^{(j)}(p),\eta^{(j+1)}(p)) - H(\eta^{(j)}(p_\Lambda),\eta^{(j+1)}(p_\Lambda))).$$

Let $\eta \in h^*$ (h: the Cartan subalgebra of $A_n^{(1)}$) and δ be the null root of $A_n^{(1)}$. We further define

$$P(\Lambda)_\mu = \{p \in P(\Lambda) \mid p^{(1)} - \omega(p)\,\delta = \mu\}, \qquad P^{(m)}(\Lambda)_\mu = P^{(m)}(\Lambda) \cap P(\Lambda)_\mu .$$

Then we have by definition

$$q^{-\omega_m(\Lambda)} f_m\,(p_\Lambda^{(m+1)} - a, \eta^{(m+1)}(p_\Lambda)\,;\,q) = \sum_{i=0}^{\infty} \#\,(P^{(m)}(\Lambda)_{a-i\delta})\,q^i,$$

$$\omega_m(\Lambda) = \sum_{j=1}^{m} jH\,(\eta^{(j)}(p_\Lambda), \eta^{(j+1)}(p_\Lambda)).$$

Let $L(\Lambda)$ be the irreducible highest weight module with the highest weight Λ and set $L(\Lambda)_\mu = \{v \in L(\Lambda) \mid hv = \mu(h)v \text{ for } h \in \mathfrak{h}\}$. Then our theorem is

Theorem. $\dim L(\Lambda)_\mu = \#\,(P(\Lambda)_\mu)$.

We conjecture that this kind of equalities holds for other solvable vertex models related to affine Lie algebras and higher representations (for the precise statement we again refer to [1]).

As a result we have

$$\lim_{m\to\infty} q^{-\omega_m(\Lambda)} f_m\,(p_\Lambda^{(m+1)} - a, \eta^{(m+1)}(p_\Lambda)\,;\,q) = \sum_i \dim L(\Lambda)_{a-i\delta}\,q^i.$$

The right hand side is nothing but the *string function* of Kac-Peterson. They showed string functions enjoy nice *modular property*. Finally the LSP itself is given as

$$P(a|\Lambda) = \sum_i \dim L(\Lambda)_{a-i\delta}\,x^{-\langle a-i\delta,\rho\rangle} \Big/ \sum_\mu \dim L(\Lambda)_\mu\,x^{-\langle\mu,\rho\rangle}, \; \rho = \Lambda_0 + \ldots + \Lambda_n.$$

There are also *face models* related to these vertex models whose local states are *dominant integral weights of a fixed level (say ℓ)* and whose Boltzmann weights are parametrized by elliptic theta functions. The 1D configuration sums X_m of these face models are obtained from those of vertex models by folding them by the action of affine Weyl groups. Their limit coincide with the *branching coefficients* for the pairs of affine Lie algebras, like $(A_n^{(1)} \oplus A_n^{(1)}, A_n^{(1)})$. Namely we consider the tensor product $L(\xi) \otimes L(\eta)$, where ξ, η are dominant integral weights of level ℓ-1, 1, and decompose it by the diagonal action. In terms of characters this amounts to $\chi_\xi \chi_\eta = \sum_a b_{\xi\eta a} \chi_a$ (level a = ℓ). The limits of X_m's coincide $b_{\xi\eta a}$'s.

References:

[1] E. Date, M. Jimbo, A. Kuniba, T. Miwa, M. Okado: One dimensional configuration sums in vertex models and affine Lie algebra characters (RIMS preprint, Kyoto University (June 1988))

[2] E. Date, M. Jimbo, A. Kuniba, T. Miwa, M. Okado : A new realization of the basic representation of $A_n^{(1)}$ (RIMS preprint, Kyoto University (June 1988))

Title: *Hecke action on the component groups of the Néron model of the Jacobian of a modular curve*

Author: *Bas EDIXHOVEN*

Address: *Math. Inst., Budapestlaan 6, 3584 CD Utrecht, Netherlands*

Pour N un nombre entier positif soit $X_0(N)_{\mathbb{Q}}$ la courbe modulaire sur $\mathbb{Q}$ paramétrant les N-isogénies cycliques entre courbes elliptiques, et $J_0(N)_{\mathbb{Q}}$ sa jacobienne. L'algèbre de Hecke agit sur $J_0(N)_{\mathbb{Q}}$ donc aussi sur son modèle de Néron $J_0(N)$ sur $\mathbb{Z}$. Soit p un nombre premier et $\Phi_{N,p}$ le groupe de composantes de la fibre géometrique $J_0(N)_p$ de $J_0(N)$ en caractéristique p.

Dans cet article nous démontrons que pour $p > 3$ l'action de l'algèbre de Hecke sur $\Phi_{N,p}$ est "Eisenstein". Cela veut dire que pour tout nombre premier ℓ ne divisant pas N l'opérateur de Hecke T_ℓ agit sur $\Phi_{N,p}$ par multiplication par $\ell+1$ (cf. [Ma], p.95). Ce résultat est une généralisation d'un théorème de K. Ribet [Ri 1], [Ri 2] (Theorem 2.24), qui prouve le même résultat en supposant que la valuation de N en p est au plus 1. À dire vrai, Ribet prouve son théorème aussi pour p = 2,3. Parce que dans ce cas la méthode de Ribet est plus efficace nous nous restreindrons au cas $p > 3$.

Pour prouver son théorème Ribet utilise la description donnée par A. Grothendieck [Gro 1] des groupes $\Phi_{N,p}$ en termes de l'accouplement de monodromie sur le groupe de caractères de la partie torique de la réduction (semistable) de $J_0(N)$ sur $\mathbb{Z}_p$. En se servant des résultats de [De-Ra] sur la réduction de $X_0(N)$ modulo p il obtient une description combinatoire de $\Phi_{N,p}$ en termes de points supersinguliers en caractéristique p. Ce qui reste alors à démontrer est une proposition sur les automorphismes des courbes elliptiques supersingulières.

Comme la méthode de Ribet ne marche qu'en cas de réduction semistable nous nous servons de la description donnée par M. Raynaud [Ray] des groupes $\Phi_{N,p}$ en termes de modèles sur $\mathbb{Z}$ des $X_0(N)_{\mathbb{Q}}$ qui sont réguliers. De tels modèles sont connus dans le cas où la valuation en p de N est au plus 1 [De-Ra], et dans le cas où $p > 3$ [Ed]. Pour ℓ un nombre premier ne divisant pas N il faut montrer que l'opérateur de Hecke T_ℓ est défini en termes des deux morphismes standards de $X_0(N\ell)_{\mathbb{Q}}$ vers $X_0(N)_{\mathbb{Q}}$. Afin de calculer l'action de T_ℓ sur $\Phi_{N,p}$ nous étendons ces deux morphismes à certains modèles convenables sur $\mathbb{Z}_p$. Ces calculs nous conduisent à démontrer la proposition (déjà prouvée par Ribet dans le cas supersingulier) mentionnée plus haut (cf. Lemme 2 de (4.2)).

L'intérêt de ce théorème de Ribet est le rôle qu'il joue dans [Ri 2], où il est démontré que la conjecture de Taniyama et Weil implique celle de Fermat. La question sur la généralisation traitée dans cet article semble avoir été posée par Mazur lors d'un exposé de Ribet sur [Ri 2]. Signalons toutefois qu'il reste encore à généraliser aux cas $p = 2,3$.

Il est peut-être utile de remarquer que dans la démonstration que Taniyama-Weil implique Fermat [Ri 2] on n'a besoin que d'une version faible du théorème de Ribet. Cette version dit que l'action de l'algèbre de Hecke sur le sous-groupe de q-torsion de $\Phi_{N,p}$ est Eisenstein pour tout nombre premier $q > 3$. D'après Mazur et Rapoport [Ma-Ra] ce sous-groupe est cyclique et on a un générateur explicite: c'est un multiple de $Z - Z'$ (dans leur notation). Il est très facile de calculer l'action d'un T_ℓ sur $Z - Z'$. Malheureusement il faut aussi remarquer qu'il y a quelques petites erreurs dans les calculs de [Ma-Ra] (cf. (4.4.1)), mais l'argument de cet alinéa reste valable. Bien sûr, il n'est pas utile d'affaiblir le théorème de Ribet quand il s'agit des conjectures de Serre.

J'aimerais remercier K. Ribet de m'avoir demandé si la généralisation de son théorème était vraie, de m'avoir envoyé une version préliminaire de son article [Ri 1], de m'avoir stimulé d'écrire ce texte, et de ses commentaires.

References:

[De-Ra] Deligne, P., Rapoport, M.: Les schémas de modules de courbes elliptiques. Lecture Notes in Mathematics 349, 143-316 (1973)

[Ed] Edixhoven, S.J.: Minimal resolution and stable reduction of $X_0(N)$. University Utrecht Dept. Math. preprint Nr. 438 (1986)

[Gro 1] Grothendieck, A.: Modèles de Néron et monodromie. Séminaire de Géométrie Algébrique 7, Exposé IX, Lecture Notes in Mathematics 288, 313-523 (1972)

[Ma] Mazur, B.: Modular curves and the Eisenstein ideal. Publications Mathématiques de l'IHES 47, 33-186 (1977)

[Ma-Ra] Mazur, B., Rapoport, M.: Behaviour of the Néron model of the Jacobian of $X_0(N)$ at bad primes. Appendix of [Ma]

[Ray] Raynaud, M. Spécialisation du foncteur de Picard. Publications Mathématiques de l'IHES 38, 27-76 (1970)

[Ri 1] Ribet, K.A.: On the component groups and the Shimura subgroup of $J_0(N)$. Séminaire de théorie des nombres de Bordeaux 1988

[Ri 2] Ribet, K.A.: On modular representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. MSRI preprint Nr. 06420-87 (1987)

Title: *The Schottky Problem*

Author: *Gerard VAN DER GEER*

Address: *Math. Inst., Amsterdam University, Roetersstraat 15,*
1018 WB Amsterdam, Netherlands

The Schottky problem asks for characterizations of jacobian varieties among all principally polarized abelian varieties. Schottky worked on this question (which goes back to Riemann (1857)). This talk deals with a set of possible answers - most of them recent - all related with Schottky's original approach.

Let (A,Θ) be a principally polarized abelian variety (ppav) over a field of characteristic $\neq 2$. Let $L = \mathcal{O}(\Theta)$. Let T be the theta group of $L^{\otimes 2}$. The space $H^0(A,L^{\otimes 2})$ has dimension 2^g. After choosing an isomorphism of the theta group T with the Heisenberg group which is the identity on the scalars k^* we can identify this space with the Schrödinger representation U_g of the Heisenberg group $H = H(g)$. (Here $g = \dim(A)$). In particular, we have a canonical basis ϑ_σ, $\sigma \in (\mathbb{Z}/2)^g$ (the so-called second order theta functions).

The sections of $L^{\otimes 2}$ define a morphism

$$F_A : A \to \mathbb{P}(U_g).$$

If the theta divisor Θ is irreducible then the degree of F_A is two and the image of F_A is the Kummer variety of A.

Let A_g (resp. $A_g(2,4)$) be the moduli space of ppav (resp. ppav with an isomorphism of T with H) of dimension g. We have a morphism

$$F : A_g(2,4) \to \mathbb{P}(U_g) \text{ with } F([A]) = F_A(0).$$

Let RA_g (resp. $RA_g(2,4)$) be the moduli space of principally polarized abelian varieties of dimension g (resp. the same with an isomorphism of T with H) plus a non-zero point of order 2 (resp. of order 4). There is a natural morphism

$$G : RA_g(2,4) \to \mathbb{P}(U_{g-1})$$

which gives for an abelian variety A plus some structure the position of the image of the non-zero point of order 4 (say b) under F_A. This point lies in a fixed space $\mathbb{P}(U_{g-1})$ of $2b$ in $T/k^* \cong A[2]$.

Forgetting the level we find morphisms

$$F' : A_g \to \mathbb{P}(U_g) / G_g$$
$$G' : RA_g \to \mathbb{P}(U_{g-1}) / G_{g-1},$$

where G_g is the Galois group of $A_g(2,4)$ over A_g.

In case A is a jacobian $\mathrm{Jac}(C)$ something special happens. Let a be a non-zero point of order two and let $\tilde{C} \to C$ be the associated double cover. If $P = (\ker [\ \mathrm{Nm}:\mathrm{Jac}(\tilde{C}) \to \mathrm{Jac}(C)])^0$ is the Prym variety of $\tilde{C} \to C$ (this is a ppav of dimension $g-1$ if g = genus of C) then

$$G'([A,a]) = F'([P]). \qquad \text{(Schottky-Jung)}.$$

Schottky's idea was that this should only happen for jacobians. More precisely, one defines a Schottky locus in RA_g by

$$RS_g := G'^{-1} \text{ (Image of F')},$$

and similarly, one defines a Schottky locus in A_g by

$$S_g = \{[A] \in A_g : \forall\, a \in A\,[2],\ a \neq 0,\ [A,a] \in RS_g\ \}.$$

Let J_g be the (closure of the) jacobian locus in A_g. It is known that J_g is an irreducible component of S_g (by van Geemen) and that RJ_g (jacobians with a non-zero point of order two) is an irreducible component of RS_g. One conjectures $J_g = S_g$ (which would give an answer to the Schottky problem). Donagi showed that RS_g contains other components than just RJ_g. In order to state a precise conjecture, first note that the Satake compactification of RA_g has three irreducible boundary components (isomorphic to A_{g-1}, RA_{g-1}, A_{g-1} and denoted by ∂^{I}, ∂^{II} and ∂^{III}). Donagi conjectured that in a toroidal compactification $\overline{RA}_g$ of RA_g one should have:

Conjecture: $\overline{RS}_g = \overline{RJ}_g \cup \partial^{I}\ \overline{RA}_g \cup (\overline{RC} \times \overline{A}_{g-5}) \cup (\cup_{k\geq 4} \overline{RJ}_{g-k} \times \overline{A}_k)$,

where $\overline{RC}$ is the closure of the locus of intermediate jacobians of cubic threefolds with an "even" point of order two.

The philosophy here is simply that one throws in at the right hand side everything that one knows of as being contained in $\overline{RS}_g$. (One is willing to adapt the conjecture if there turns out to be more!) However, the merit of this conjecture is that it implies various other conjectures made in relation with the Schottky problem and explains their relationship.

The first Corollary of the Conjecture is : $S_g = J_g$.

By looking at the boundary of the moduli space one finds the following conjectures. Define

$$\Gamma_{00} = \{s \in H^0(A, L^{\otimes 2}) : m_0(s) \geq 4\},$$

where m_0 denotes the multiplicity at the origin. Let $V(\Gamma_{00})$ be the set of common zeroes of the sections of Γ_{00}. One assumes Θ to be irreducible.

1) If $A = \mathrm{Jac}(C)$ then $V(\Gamma_{00}) = C - C$ for $g \neq 4$ (plus two points if $g=4$).

2) If A is not a jacobian then $V(\Gamma_{00}) = \{0\}$.

3) If $A = \mathrm{Jac}(C)$ then $F_A(A) \cap F(\bar{A}_g(2,4)) = F_A(\frac{1}{4}(C-C))$.

4) If A is not a jacobian then $F_A(A) \cap F(\bar{A}_g(2,4)) = F_A(0)$.

5) Let $\tilde{C} \rightarrow C$ be a double unramified cover with Prym variety P. Both P and $\mathrm{Jac}(\tilde{C})$ map to $\mathbb{P}(U_{g-1})$, the first by F_A and the second by $F_{\mathrm{Jac}(\tilde{C})}$ followed by a projection.

The intersection of the images is the image of $S^2\tilde{C}/i$ with i the involution associated to $\tilde{C} \rightarrow C$.

The behaviour at ∂^I gives 1) and 2), the behaviour at ∂^{III} gives 3) and 4), while the behaviour at ∂^{II} gives 5).

Conjectures 1),...,4) were already made several years ago in [vG-vdG], independently of the above approach. Their status is : 1) is now Welters' theorem; 2) is true for the intermediate jacobians of cubic threefolds (Donagi-vdG) and for $g \geq 14$ we know that $V(\Gamma_{00})$ is finite for the generic abelian variety [B-D-D-vdG]; 3) is known for $g=3$ [vG-vdG] and for $g=4$ [Donagi]; 4) is known for $g=4$ [Donagi]. These results give evidence at the boundary for Donagi's Conjecture.

One can also consider infinitesimal versions of conjecture 2). This leads to : (assume $k = \mathbb{C}$)
Conjecture: An indecomposable ppav is a jacobian if and only if we have a differential equation of the form

$$(D_1^4 + \text{lower order terms})\ \vec{\vartheta}(\tau,z)|_{z=0} = 0,$$

where $D_1^4 + \ldots$ is a polynomial in constant vector fields with $D_1 \neq 0$ and $\vec{\vartheta}$ is the vector of theta functions $\vartheta_\sigma(\tau,z)$.

This conjecture is stronger than Novikov's Conjecture which one gets by replacing $(D_1^4 + \ldots)$ by a specific polynomial

$$D_1^4 - D_1D_3 + D_2^2 + d.$$

(The K-P equation). This conjecture was solved by Shiota (in the affirmative sense).

The above conjectures are also related to trisecant properties of the Kummer variety. Other relations can be obtained by studying Γ_{00} as A tends to a rank-1 degeneration.

References:

[B-D-D-vdG] A. Beauville, O. Debarre, R. Donagi, G. van der Geer: Note to appear in C.R.

[Donagi] R. Donagi: The Schottky Problem. Preprint MPI 1987

[vG-vdG] B. van Geemen, G. van der Geer: Kummer varieties and the moduli space of abelian varieties. Am. J. of Math. 108(1986)

Title: *Supersingular abelian surfaces and automorphism groups of lattices*

Author: *Tomoyoshi IBUKIYAMA*

Address: *Dept. Math., College of General Education, Kyushu University, Ropponmatsu, Fukuoka-City, 810 Japan*

AIM: To give a general method how to get explicit automorphism groups of all positive definite quadratic, hermitian, or quaternion hermitian forms in a given fixed genus.

MOTIVATION: Theory of supersingular abelian surfaces / char. p developed by Katsura-Oort. The above method was applied to this case where positive definite binary quaternion hermitian forms are concerned.

1. Supersingular abelian surfaces.

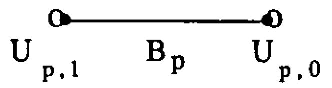
Let E be a supersingular elliptic curve / $\overline{\mathbb{F}}_p$ and put $D = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. D is the definite quaternion algebra / $\mathbb{Q}$ with discriminant p.∞. The theory of supersingular abelian surfaces (i.e. those A s.t. $A \sim E^2$) is more or less connected with the following group G:

$$G = \{ g \in M_2(D) : g\,{}^t\bar{g} = n(g)\, 1_2,\ n(g) \in \mathbb{Q}^{>0} \}.$$

We consider three subgroups of G_A of the form

$$U = G_\infty \times (\prod_{q \neq p} U_q) \times P,$$

where $U_q = G_q \cap GL_2(\mathcal{O}_q)$ ($\mathcal{O}$: maximal order of D) and $P = U_{p,0}$, $U_{p,1}$ or $B_p \subset G_p$ (the standard parahoric subgroups of G_p).



$$U_{p,1} = G_p \cap GL_2(\mathcal{O}_p)$$

We denote these groups by $\mathfrak{U}_1, \mathfrak{U}_0$, B according as $P = U_{p,0}$, $U_{p,1}$, B_p. Each group $\mathfrak{U}_1$, or $\mathfrak{U}_0$ corresponds to principal, or non principal genus of maximal lattices in D^2, respectively.

1) (Serre) (principal polarizations on E^2) / Aut $(E^2) \cong \mathfrak{U}_1 \backslash G_A / G$ (bijective).

2) (Katsura-Oort) (the set of irreducible components of A_s) $\cong$ $\mathfrak{U}_0\backslash G_A/G$,where A_s is the locus of supersingular abelian surfaces in $A_{2,1}$.

3) Take a component V of A_s which corresponds to $\mathfrak{U}_0 h G$, and principal polarization C on E^2 which corresponds to $\mathfrak{U}_1 gG$. Then, (E^2,C) is on V, if and only if $\mathfrak{U}_0 h G \cap \mathfrak{U}_1 g G \neq \emptyset$. $B\backslash G_A/G$ has also some geometrical meaning, but omitted here.

Not only the class number of $\mathfrak{U}$ (i.e. the number of double cosets in $\mathfrak{U}\backslash G_A/G$), but also the unit group of each class has geometrical meaning. Here, for the decomposition $G_A = \coprod \mathfrak{U} g_i G$, $\Gamma_i := g_i^{-1} \mathfrak{U} g_i \cap G$ is called unit group. For example, Aut (E^2,C), or decomposition group of V in $A_{2,1,2}$ is given by the unit groups of $\mathfrak{U}_1$, or $\mathfrak{U}_0$, respectively.

2. Number theory (new mass formula) .

We consider the following general problems:

Let D be either the rational number field, a imaginary quadratic field, or a definite quaternion algebra over $\mathbb{Q}$. Let V be a finite dimensional vector space / D and take a (hermitian) metric h with respect to the unique positive involution of D on V. We assume that h is positive definite. From a given genus $\mathfrak{L}$ of $\mathfrak{O}$-lattices in V, denote by $L_1,\ldots,L_H$ a set of complete representative of classes in $\mathfrak{L}$, and put $\Gamma_i = \mathrm{Aut}\,(L_i)$ (metric preserving automorphisms).

Problem 1 : Calculate H.

Problem 2 : For a given finite group Γ, count the number of Γ_i such that $\Gamma_i \cong \Gamma$.

It is more or less known how to solve *Problem 1* (Eichler, Selberg, Tamagawa, Hashimoto). The method is trace formula, or a kind of mass formula. But *Problem 2* is fairly different from *Problem 1* in nature. Roughly speaking, *Problem 1* is a problem on linear representation, but *Problem 2* is on permutation representation, and permutation representation is not determined by linear representation attached to it. So, we need a new formula, which is a generalization of known formula by Hashimoto. Let r be a natural number. Embed G diagonally into G^r and regard G as a subgroup of G^r. For $\gamma \in G^r$, denote by $\{\gamma\}_G$ the G-conjugacy class of γ. Put

$$m\,(\{\gamma\}_G, \mathfrak{L}) = \sum_{i=1}^{H} \frac{\#\,(\Gamma_i^r \cap \{\gamma\}_G)}{\#\,(\Gamma_i)}$$

Theorem. There is a formula which tells us how to calculate $m(\{\gamma\}_G, \mathfrak{L})$. Using this "new" masses, we can solve *Problem 2* by some induction steps. (We omit details here).

For example:

Theorem. As for $\mathcal{U}_0$ in §1, $\Gamma_i/\{\pm 1\}$ is isomorphic to one of the following groups: $\{1\}, \mathbb{Z}/2, \mathbb{Z}/3, (\mathbb{Z}/2)^2, S_3, A_4, S_4, D_{12}, A_5$.
For all p, the number of Γ_i s.t. $\Gamma_i \cong \Gamma$ (Γ : one of the above) is explicitly given. (For $p \leq 31$, this was obtained by Katsura-Oort by a geometric method).

Title: *Quotients of abelian surfaces in characteristic p*

Author: *Toshiyuki KATSURA*

Address: *Dept. Math., Ochanomizu University, 2-1-1 Otsuka,*
Bunkyo-ku, Tokyo, 112 Japan

Let k be an algebraically closed field of characteristic p, and let X be an algebraic variety of dimension n over k. X is called a rational variety, if X is birationally equivalent to the projective space $\mathbb{P}^n(k)$ of dimension n. X is called a unirational variety, if there exists a generically surjective rational mapping φ from $\mathbb{P}^n(k)$ to X. In particular, if there exists a purely inseparable rational mapping φ of degree p from $\mathbb{P}^n(k)$ to X, we call X a Zariski surface. By definition, if X is rational, then X is unirational. If $n = 1$, by Lüroth's theorem, the converse holds. If $n = 2$ and char $k = p = 0$, by Castelnuovo's criterion of rationality, the converse also holds. However, if $n = 2$ and char $k = p > 0$, the converse does not necessarily hold. The first counterexample was given by Zariski in 1958. We want to know the characterization of unirational surfaces in positive characteristic.

Proposition (Properties of unirational varieties). Let X be a non-singular complete unirational variety. Then, we have the following:

1) $q(X) :=$ dimension of the Albanese variety of $X = 0$,
2) X is supersingular, i.e. the Picard number $\rho(X)$ of X is equal to the second Betti number $b_2(X)$ (Shioda),
3) the algebraic fundamental group $\pi_1^{alg}(X)$ is a finite group (Serre),
4) the order of $\pi_1^{alg}(X)$ is prime to p (Katsura, Crew, Ekedahl).

From the view point of classification theory, we have the following:

Kodaira dimension K(X)		p = 0	p > 0
$-\infty$	rational	+	+
	irrational ruled	-	-
0	abelian	-	-
	hyperelliptic (quasi-hyperelliptic)	-	-
	K3	-	+
	Enriques	-	+
1	elliptic (quasi-elliptic)	-	+
2	of general type	-	+

where + means that the class contains unirational surfaces, and - means that the class does not contain unirational surfaces. We have examples of unirational surfaces for the classes of + sign.

Now we are interested in K3 surfaces. We have the following conjecture to characterize the unirational K3 surfaces.

Conjecture: (Artin and Shioda). For a K3 surface X, X is unirational if and only if X is supersingular.

The "only if" part follows from Proposition 2). If $p = 2$, then this conjecture is affirmative (Rudakov-Shafarevich). Now, assume $p \geq 3$. Let A be an abelian surface. Then for a Kummer K3 surface Km(A), the conjecture is also affirmative (Shioda). We can give a new proof of this result, using the locus of supersingular abelian surfaces in the fine moduli scheme of principally polarized abelian surfaces with level n-structure ($n \geq 3$, $(n,p) = 1$).

Let G be a finite subgroup of $\mathrm{Aut}_v(A)$, where $\mathrm{Aut}_v(A)$ is the automorphism group of A as an algebraic surface. If A / G is birationally equivalent to a K3 surface, we call the minimal non-singular model of A / G a generalized Kummer surface, and denote it by Km(A,G). We can classify such subgroups G for $p \geq 7$ or $p = 0$. Assume $p \geq 7$. Then, we can show that Km(A,G) is unirational if and only if Km(A,G) is supersingular. This result supports Artin-Shioda's conjecture. In case A is isomorphic to a product of two supersingular elliptic curves, we can show that Km(A) is a Zariski surface, if $p \not\equiv 1$ mod. 12, using a result on generalized Kummer surfaces.

Title: *Primality Testing*

Author: *H.W. LENSTRA, Jr.*

Address: *Dept. Math., University of California, Berkeley, CA 94720,*
U.S.A.

In this lecture an outline is given of the proof of the following theorem, which is due to Adleman and Huang, after earlier work by Goldwasser and Kilian:

Theorem. *The set of primes can be recognized in random polynomial time. The statement means that there exists a function* $f : \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \to \{0,1\}$ *such that:*

1) *there exists an algorithm calculating* $f(n,r)$ *in time* $(\log(n+r))^{O(1)}$;
2) $f(n,r) = 1 \Rightarrow n$ *is prime;*
3) *there exists* $c > 0$ *such that:*
   n *is prime* $\Rightarrow \#\{r : f(n,r) = 1$ *and* $(\log r) \le (\log n)^c\}$
   $\ge \frac{1}{2} \cdot \#\{r : (\log r) \le (\log n)^c\}$.

One should think of n as the number to be tested for primality; of r as a long sequence of "random bits"; of the output "$f(n,r) = 1$" as " n is prime"; and of the output "$f(n,r) = 0$" as "I do not know".

In principle, an algorithm as this can be used to test n for primality, as follows. Pick r, $\log r \le (\log n)^c$, at random; and calculate $f(n,r)$. If $f(n,r) = 1$ then n is prime, and one stops. Otherwise (if $f(n,r) = 0$), repeat with a different value of r. If this is done k times, and each time $f(n,r) = 0$, then it is for large k quite unlikely that n is prime, since by 3) one expects $f(n,r) = 1$ pretty soon, if n is prime. So in that case one is led to expect that n is composite. To be sure, one can then run a compositeness test, which has the same properties as above, but with "prime(s)" replaced by "composite (numbers)". Such a compositeness test has been known for a long time (Solovay-Strassen, Rabin).

Goldwasser and Kilian *almost* proved the above theorem, using the following result:

Theorem. *Let* $n \in \mathbb{Z}$, $n > 1$, $\gcd(n,6) = 1$. *Suppose there exist an elliptic curve* $E : Y^2 = X^3 + aX + b$ *over* $\mathbb{Z}/n\mathbb{Z}$, *a point* $P = (x : y : 1) \in E(\mathbb{Z}/n\mathbb{Z})$, *and an integer* q *such that*

$$q \cdot P = 0 = (0 : 1 : 0), \quad q > (n^{1/4} + 1)^2.$$

Then: q *prime* $\Rightarrow n$ *prime.*

Proof. Let p|n be prime. The image $\bar{P}$ of P in $E(\mathbb{F}_p)$ is non-zero, so $\bar{P}$ has order q. Hence $(n^{1/4}+1)^2 < q \le \# E(\mathbb{F}_p) < (\sqrt{p}+1)^2$, so $p > \sqrt{n}$, and n is prime.

The algorithm of Goldwasser and Kilian now runs as follows. Whenever the algorithm to be described needs a "random number", one should use a beginning segment of the binary representation of r for this purpose; this beginning segment is then "removed" from r. This is the only rôle played by r.

Step I. Draw $a,b \in \mathbb{Z}/n\mathbb{Z}$ at random, and let E be the corresponding elliptic curve.

Step II. Use an algorithm of Schoof to determine a number m such that *if* n is prime *then* $\#E(\mathbb{F}_n) = m$, and $m \le (\sqrt{n}+1)^2$.

Step III. Check whether m factors as $m = k \cdot q$, where k is the product of all small ($\le (\log n)^{cst}$, say) prime factors of m that one can find, $k \ge 2$, $q > (n^{1/4}+1)^2$, and q is "probably" prime (as indicated by running a compositeness test on q).

If m does *not* factor in this way, go back to step I.

Step IV. Draw $P' \in E(\mathbb{Z}/n\mathbb{Z})$ at random (this can be done, if n is prime), until one is found for which $P = k \cdot P'$ is of the form $(x : y : 1)$ (if n is prime this should happen very soon). Check that $qP = 0$ (if $qP \ne 0$ then n cannot be prime!).

Step V. Prove recursively that q is prime. (The depth of the recursion is logarithmic, since $q \le m/2 \lesssim n/2$).

If all steps have been completed successfully one announces that n is prime (f(n,r) = 1). If one gets stuck, one spends too much time, one gives up (f(n,r) = 0).

That this algorithm satisfies 2) follows from the last theorem. The difficulty is to prove 3). This comes down to proving that for prime n there are "many" $(\ge \frac{n^2}{(\log n)^{0(1)}})$ pairs a,b giving rise to an elliptic curve E for which $\#E(\mathbb{F}_n)$ is prime. By results of Deuring (giving the number of elliptic curves E for which $\#E(\mathbb{F}_n)$ equals a given number) this is essentially equivalent to proving that intervals of the type $(x, x+\sqrt{x})$ contain "many" primes $(\ge \frac{\sqrt{x}}{(\log x)^{0(1)}})$ for all sufficiently large x. This is a well known open problem; so with the present status of analytic number theory the Goldwasser-Kilian algorithm is not sufficient to prove the theorem. One *can* prove, however, that the algorithm recognizes *most* primes, the number of exceptions (to 3)) $\le x$ being $\le x^{\frac{15}{16}-\varepsilon}$ for some $\varepsilon > 0$ and all sufficiently large x.

To get around this problem, Adleman and Huang consider abelian varieties A over $\mathbb{Z}/n\mathbb{Z}$ of dimension 2. If n is prime, then $\#A(\mathbb{F}_n)$ lies in an interval of length $\approx 8n^{3/2}$ around n^2 ; such an interval, which is like $(x, x + x^{3/4})$, *does* contain enough primes for all x, by a result of Iwaniec and Jutila. This eliminates the analytic number theory problem, but it creates many new ones. The most serious one is the following: the obvious analogue of the second theorem above for abelian *surfaces* has the condition $q > (n^{1/4} + 1)^2$ replaced by $q > (n^{1/4} + 1)^4$; so the induction is going the wrong way! And in fact, if one uses abelian surfaces just as Goldwasser-Kilian use elliptic curves, then q will usually be $\approx n^2$, so with twice as many digits as n. Adleman and Huang solve this apparently definitive obstacle as follows: apply the "wrong induction" (replacing n by q) *three* times, so that the primality proof for n has been reduced to the primality proof for a number $\approx n^8$: a number that is much bigger, but that has the advantage of being *random* to a certain extent, so that one is entitled to expect that the Goldwasser-Kilian algorithm is able to deal with it!

Other problems turn up as well if one transposes the Goldwasser-Kilian method to abelian surfaces. Here are some changes that have to be made.

In step I, one must now choose a "random" abelian surface. Adleman and Huang do this by picking $f \in (\mathbb{Z}/n\mathbb{Z})[X]$ of degree 6 at random, and letting A be the Jacobian of $Y^2 = f(X)$.

In step II, one must replace Schoof's algorithm by a generalization to all abelian varieties that is due to J. Pila.

In step III and IV a simplification occurs: one may take $k = 1$, so that m itself is to be subjected to the compositeness test, and $P = P'$.

Step V, as already remarked, should only be applied three times, after which one changes to the elliptic curve method.

The final difficulty that Adleman and Huang had to master was the proof of 3). The problem here is the unavailability of results analogous to those of Deuring for elliptic curves. Adleman and Huang prove rather weak analogues of Deuring's results, which are just sufficient for their purposes.

Title: *Isogenies of Elliptic Curves*

Author: *D.W. MASSER*

Address: *Dept. Math., University of Michigan, Ann Arbor,
Michigan 48109, U.S.A.*

Let k be a number field, and for a Weierstrass elliptic curve $E : y^2 = 4x^3 - g_2 x - g_3$ defined over k write

$$w(E) = \max (h(g_2), h(g_3), 2)$$

where h denotes the logarithmic absolute Weil height. We discussed the following results.

Theorem *(D.W. Masser, G. Wüstholz). Given an integer* $d \geq 1$, *there exists an effective constant* c, *depending only on* d, *with the following property. Let* k *be a number field of degree at most* d, *and suppose* E, E* *are elliptic curves over* k *that are* k-*isogenous. Then there is a* k-*isogeny between them of degree at most* $c(w(E))^4$.

Corollary 1. *The number of* k-*isomorphism classes of elliptic curves over* k *that are* k-*isogenous to* E *is at most* $c_1 (w(E))^8$.

Corollary 2. *Each such isomorphism class contains an elliptic curve* E* *with* $w(E^*) \leq c_2\, w(E)$.

For a prime ℓ let E_ℓ be the group of ℓ-division points of E, and write G_ℓ for the Galois group of $k(E_\ell)$ over k.

Corollary 3. *Suppose* $\ell > c_3(w(E))^4$. *Then the action of* G_ℓ *on* E_ℓ *is semisimple. Further, if* E *has no complex multiplication, the action is irreducible.*

This last corollary implies an effective version of a result of Bashmakov. Namely, for $d \geq 1$, $m \geq 1$ there is an effective constant C, depending only on d and m, with the following property. Let $P_1,\ldots,P_m$ be independent points on E(k) with logarithmic Weil heights bounded above by some $U \geq 1$. Let H_ℓ be the Galois group of $k(E_\ell; \frac{P_1}{\ell},\ldots,\frac{P_m}{\ell})$ over $k(E_\ell)$. Then H_ℓ is isomorphic to E_ℓ^m provided

$$\ell > C \max \{(w(E))^4, (w(E))^{\frac{3m}{2}} U^{\frac{m}{2}} \}.$$

The proof of the main Theorem uses Baker's method in transcendental number theory applied to the algebraic group $E^2 \times E^{*2}$.

Title: *Supersingular abelian varieties*

Author: *Frans OORT*

Address: *Math. Inst., Budapestlaan 6, 3508 TA Utrecht, Netherlands*

1. Introduction.

We try to obtain information about moduli spaces of abelian varieties by studying stratifications. We shall exploit extra structure in positive characteristics.

We mention a general idea:

Strategy: a) Find some "good" stratification $A = \cup W_\alpha$, $\alpha \in I$; index set partially ordered by $\alpha > \beta \Leftrightarrow W_\beta \subset \overline{W}_\alpha$ such that:

b) $\exists!$ last one W_{last} ("easy...?") and

c) describe every $\overline{W}_\alpha$ in the neighbourhood of points of W_{last}.

We give some properties based on earlier joint work with Tadao Oda (1977), with P. Norman (1980) and with T. Katsura (1985 ~ 1987); we use methods by M. Eichler (1937 ~ 1955), K. Hashimoto and T. Ibukiyama (1980 ~ 1983), and L. Moret-Bailly (1981 ~ 1985).

Several ideas of this talk stem from joint efforts with T. Ekedahl (on stratifications), and with Ke-Zheng Li (on polarized flag type quotients).

Notation: All fields considered contain $\mathbb{F}_p$.

2. Stratification by p-rank.

Notation: If X is an abelian variety, then $f(X) = f$, if $X[p](\bar{k}) \cong (\mathbb{Z}/p)^f$ with $X[n] := \text{Ker}(\times n : X \to X)$. Fix $g \in \mathbb{Z}_{>0}$, $A_{g\ldots} \supset V_i = \{[(X,\ldots)] \mid f(X) \leq i\}$. Note that $0 \leq f \leq \dim X$ (and all values appear), hence $V_0 \subset \ldots \subset V_i \subset V_{i+1} \subset \ldots \subset V_g = A_{g\ldots}$. We say that an elliptic curve E is supersingular, if $f(E) = 0$ (i.e. E has *no* geometric points of order p).

Example: $k=\bar{k}\supset\mathbb{F}_p$, # {k-isomorphism classes of $E \mid E$ is supersingular} $= h = h(p,1)$ is finite, and this number h can be computed as the class number $h = H_1\,(p,1)$ for the order $B = \mathrm{End}(E)$ (for some fixed E) in the quaternion algebra $B\otimes\mathbb{Q} = K_{p,\infty}$ ramified only at p and ∞ (Eichler, Deuring, Igusa).

Theorem (Norman, Oort). *Fix* g; *then*

$$\dim V_i = \tfrac{1}{2}g(g+1) - (g-i)$$

(all components have the same dimension, and much more is known).

Problem: Describe the stratification of A_g given by the V_i's, e.g. (ir)reducible? How do components fit together etc. ?

We show below (Ekedahl, Oort, unpublished): *Fix* $g = 2$, *fix* $n\in\mathbb{Z}_{\geq 1}$, *fix* $i = 1$; *then*

$$V_{1,n} \hookrightarrow A_{2,1,n} \textit{ is irreducible.}$$

(again: $V_{1,n}$ *is the (coarse) moduli scheme of triples* (X,λ,α), *where* $\dim X = 2$, $f(X)\leq 1$, $\lambda : X \xrightarrow{\sim} X^t$ *and* α *is a level-*n*-structure).*

3. Stratification by formal isogeny types *(fit).*

Define the p-divisible Tate group scheme by

$$\tau_p X := \varprojlim_i X\,[p^i].$$

Following Dieudonné and Manin this p-divisible group scheme can be written up to isogeny as $\tau_p X \sim (*)$, over $\bar{k}$, where

$$(*) = f(G_{1,0}+G_{0,1}) + s\,G_{1,1} + \sum_j^{<\infty} G_{(n_j,m_j)} + G_{(m_j,n_j)}$$

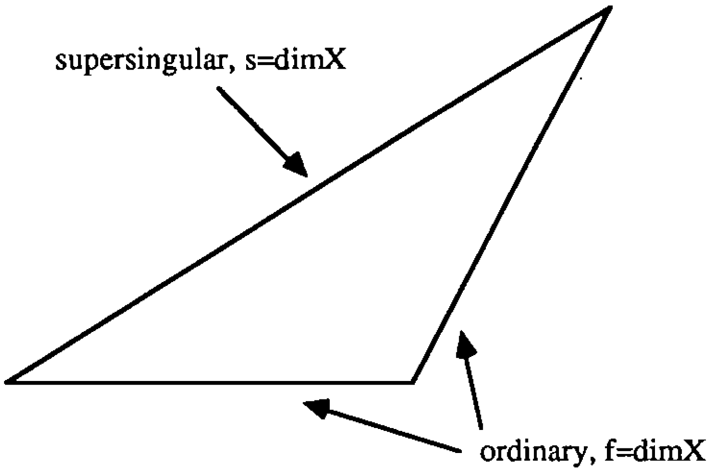
with $n_j \geq m_j \geq 1$, $(n_j,m_j) = 1$. Here $G_{a,\dots}$ is a formal group of dimension a, and $(G_{a,b})^t$ (Serre dual) $\cong G_{b,a}$. The combination

$$f((1,0) + (0,1)) + s(1,1) + \sum_j((n_j,m_j) + (m_j,n_j))$$

is called a formal isogeny type. This gives a stratification which (for $g\geq 3$) is finer than the p-rank stratification.

Example: $g = 3$: The strata given by $3\cdot(1,1)$ and by $(2,1) + (1,2)$ together make $V_0 \subset A_3$. We saw dim $(V_0, g = 3) = \frac{1}{2} 3\,(3 + 1) - (3 - 0) = 3$, but by Katsura, Oort (already Oda, Oort) dim (locus $3\cdot(1,1)$) = 2, if λ is an isomorphism, so locus $3\cdot(1,1) \subsetneq V_0$.

Remark/Question: Every *fit* gives a Newton polygon:



Under specialization, the point on the old Newton polygon goes down. Any *fit* is "between" ordinary (f = dim X) and supersingular (s = dim X). If (*) is under (*'), $\exists$? spezialization $X_\xi \to X_0$ such that $\tau_p X_\xi \sim_{\bar{k}} (*)$ and $\tau_p X_0 \sim_{\bar{k}} (*')$ (i.e. can every plausible spezialization be realized?).

4. Supersingular abelian varieties.

Theorem/Definition (Eichler, Deuring, Shioda, Deligne, Oort). $k = \bar{k} \supset \mathbb{F}_p$, E *is some supersingular elliptic curve over* k:

a) $\tau_p X \sim g\cdot G_{1,1} \Leftrightarrow E^g \sim X$ ($\overset{\text{def}}{\Leftrightarrow}$ X is supersingular).

b) $X[p] \cong (\alpha_p)^g \Leftrightarrow E^g \cong X$ ($\overset{\text{def}}{\Leftrightarrow}$ X is superspecial).

Here $\alpha_p = \mathrm{Ker}\,(F : \mathbb{G}_a \to \mathbb{G}_m)$. Note that E is supersingular iff $E[p] = \alpha_p$. Note that for $g \leq 2$ we have $f(X) = 0 \Leftrightarrow$ X is supersingular. But for $g \geq 3$, we have $f(X) = 0 \not\Leftrightarrow$ X is supersingular.

Note the curious aspect of the theorem: in general (in char. zero) a splitting of Lie X does not imply in general any splitting of X, (in char. p) a splitting of $\tau_p X$ or of the p-Lie algebra Lie X does not imply any splitting of X .

Remark (Lenstra, Oort): If $(*)$ is a *fit*, $(*) \neq g\cdot(1,1)$ then there exists an absolutely *simple* abelian variety X with $\tau_p X \sim (*)$ (so supersingular is the only exception!).

Notation: $d = d(g) = [\frac{g^2}{4}]$

$h(p,1) := H_1(p,1) = \#\{\bar{k}\text{-isomorphism classes of } E \mid E \text{ supersingular}\}$

$h(p,g) := \#(\{\mu | \mu \equiv \text{polarization on } E^g\} / \equiv) = H_g(p,1)$, g *odd*

$h(p,g) := \#(\{\mu | \mu \cong \text{polarization on } E^g, \operatorname{Ker}\mu = E^g[p]\} / \cong) = H_g(1,p)$, g *even*

($B = \operatorname{End}(E)$, $H_g(p,1)$ principal genus, ... etc.).

We denote by $\mathcal{S} \subset A_{g,1}$ the supersingular locus. One expects:

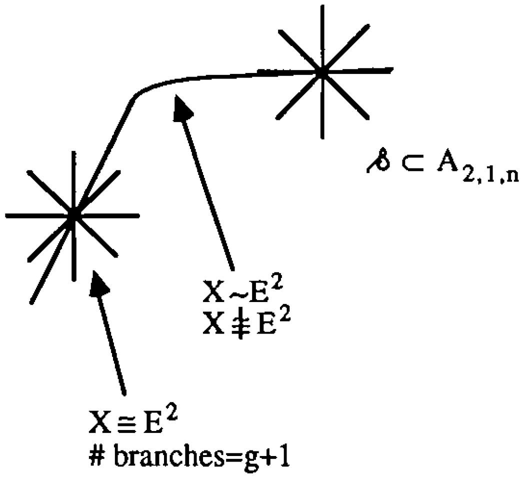
? $\dim \mathcal{S} = d(g) = [\frac{g^2}{4}]$,

$\#$ components of $\mathcal{S} = h(p,g)$.

Note: For "$p \to \infty$",
$h(p,1) \sim p/12$ (Eichler, 1937),
$h(p,2) \sim p^2/2880$ (Hashimoto, Ibukiyama, 1982),
$h(p,3) \sim p^6/2^9\cdot 3^4\cdot 5\cdot 7$ (Hashimoto, 1983).

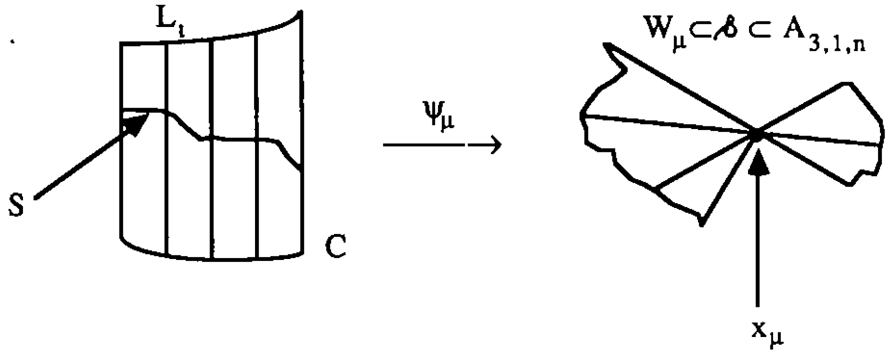
Examples: $g = 1$, ? is O.K..

$g = 2$, ? is O.K.; every component $W \subset \mathcal{S} \subset A_{2,1}$ has $\tilde{W}$ (normalization) $\cong \mathbb{P}^1$, $\#$ components $= h(p,2)$; in a fine moduli scheme $A_{2,1,n} \to A_{2,1}$ they intersect like (quite a lot is known: Katsura, Oort):



$g = 3$, ? is O.K.; construct $C := Z(X_1^{p+1} + X_2^{p+1} + X_3^{p+1}) \subset \mathbb{P}^2$, $P \to C$ the $\mathbb{P}^1$-bundle given by $P = \operatorname{Proj}(\mathcal{O}_c \oplus \mathcal{O}_c(1))$; there exists a section $S \subset P \to C$, s.t. any component $W \subset \mathcal{S} \subset A_{3,1}$ is given by μ, and $\psi_\mu : P \to W$, $\psi_\mu(S) =$

x_μ (point); no other curves are contracted for any $t \in C(\mathbb{F}_{p^2})$; along $\psi_\mu(L_t)$ many components of $\mathcal{S}$ meet, outside $\cup\ \psi_\mu(L_t)$ no other components meet W_μ; if W_μ and $W_{\mu'}$ intersect along $\psi(L)$, $\mu \neq \mu'$, then $x_\mu \neq x_{\mu'}$, etc. :



Most of these results are derived using (polarized) flag type quotients. Katsura, Li, Oort hope to be able to show that (?) is correct for $g = 4$.

Remark: $\mathcal{S} \subset A_{g,1}$ (i.e. principal polarization) is essential for results as in (?), e.g. the supersingular locus for $g = 3$, p^3 = degree (λ) has components of dimension $3 \neq 2 = [\frac{g^2}{4}]$.

Sketch of the proof of " $V_{1,n} \hookrightarrow A_{2,1,n}$ is irreducible":

a) (à la Raynaud): Show that $V_{1,n} - V_{0,n}$ is quasi-affine (use thesis of Moret-Bailly).

b) (Ekedahl): In $\mathcal{S} \subset A_{g,1,n}$ one can connect $(E^g,\lambda,\alpha) = x_0$ and $(E^g,\lambda',\alpha') = x$ by T_N, where $\psi: T_N \rightarrow \mathcal{S} \subset A_{g,1,n}$, $\psi(P_0) = x_0$, $\psi(P_N) = x$ and T_N has N components, each isomorphic to $\mathbb{P}^1$.

From a) and b) : For all components W of $V_{1,n}$ there exists some (E^g,λ,α), and $\mathcal{S}$ is connected.

c) Deformation theory at (E^g,λ), E supersingular, gives the deformation spaces by $T = \begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{pmatrix}$, with $T_{12} = T_{21}$ (without Dieudonné-modules, etc.), and $HW = T$ is the Hasse-Witt matrix. Conclude: locally at $(E^g,\lambda,\alpha) = x$, we see that V_1 is given by $\det(T) = 0$, hence locally at x invertible, and it contains $V_0 = \mathcal{S}$. Now this holds at all superspecial points.

Title: *Kolyvagin's proof of the finiteness of Mordell-Weil and Tate-Shafarevich groups of certain elliptic curves over $\mathbb{Q}$.*

Author: *Norbert SCHAPPACHER*

Address: *Max-Planck-Institut für Mathematik, Gottfried-Claren-Strasse 26, 5300 Bonn 3, Germany*

Kolyvagin's recent striking theorem was presented following very closely Karl Rubin's exposition of it in his preprint (Max-Planck-Institut für Mathematik, Bonn, July 1988) of which we take the liberty to copy the first two (out of 10) pages, as well as the final bibliography.

Introduction.

This paper gives a complete proof of a recent theorem of Kolyvagin [3,4] on Mordell-Weil groups and Tate-Shafarevich groups of elliptic curves. Let E be an elliptic curve defined over $\mathbb{Q}$, and assume that E is modular: for some integer N there is a nonconstant map defined over $\mathbb{Q}$

$$\pi : X_0(N) \to E$$

which we may assume sends the cusp ∞ to 0. Here $X_0(N)$ is the usual modular curve over $\mathbb{Q}$ (see for example [8]) which over $\mathbb{C}$ is obtained by compactifying the quotient $\mathcal{H}/\Gamma_0(N)$ of the complex upper half-plane $\mathcal{H}$ by the group

$$\Gamma_0(N) = \left\{ \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in SL_2(\mathbb{Z}) : c \equiv 0 \ (\text{modulo } N) \right\}.$$

The points of $X_0(N)$ correspond to pairs (A,C) where A is a (generalized) elliptic curve and C is a cyclic subgroup of A of order N. Fix an imaginary quadratic field K in which all primes dividing N split, and an ideal $\mathfrak{n}$ of K such that $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$. Write H for the Hilbert class field of K and x_H for the point in $X_0(N)(\mathbb{C})$ corresponding to the pair

$$(\mathbb{C}/\mathcal{O}_K, \mathfrak{n}^{-1}/\mathcal{O}_K).$$

Fix an embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}$; then the theory of complex multiplication shows that $x_H \in X_0(N)(H)$. Define $y_H = \pi(x_H) \in E(H)$, $y_K = \mathrm{Tr}_{H/K}(y_H) \in E(K)$, and $y = y_K - y_K^{\tau} \in$

E(K), where τ denotes complex conjugation on K. Let $Ш_{E/\mathbb{Q}}$ denote the Tate-Shafarevich group of E over $\mathbb{Q}$.

Theorem (Kolyvagin [3,4]). *Suppose* E *and* y *are as above. If* y *has infinite order in* E(K) *then* E($\mathbb{Q}$) *and* $Ш_{E/\mathbb{Q}}$ *are finite.*

Remarks: 1. The proof of this theorem given below is organized differently from Kolyvagin's proof, and somewhat simplified, but the important ideas are all due to Kolyvagin and contained in [3,4].

2. It is not difficult to show, using the Hecke operator w_N, that y has infinite order if and only if both y_K has infinite order and the sign in the functional equation of the L-function L(E,s) is + 1.

3. The proof will give an annihilator of $Ш_{E/\mathbb{Q}}$ which, via the theorem of Gross and Zagier [2], gives evidence for the Birch and Swinnerton-Dyer conjecture.

4. Observe that Kolyvagin's theorem makes no mention of the L-function of E. To relate his result to the Birch and Swinnerton-Dyer conjecture one needs the following:

Theorem (Gross and Zagier [2]). *With* E *and* y *as above,* y *has infinite order in* E(K) *if and only if* $L(E,1) \neq 0$ *and* $L'(E,\chi_K,1) \neq 0$, *where* χ_K *is the quadratic character attached to* K.

Analytic Conjecture. *If* E *is a modular elliptic curve and the sign in the functional equation of* L(E,s) *is* +1, *then there exists at least one imaginary quadratic field* K, *in which all primes dividing* N *split, such that* $L'(E,\chi_K,1) \neq 0$.

This analytic conjecture, as yet unproved, together with the theorems of Kolyvagin and Gross and Zagier, would imply:

(*) *For any modular elliptic curve* E, *if* $L(E,1) \neq 0$ *then* E($\mathbb{Q}$) *and* $Ш_{E/\mathbb{Q}}$ *are finite.*

Assertion (*) is known for elliptic curves with complex multiplication, by theorems of Coates and Wiles [1] (for E($\mathbb{Q}$)) and Rubin [6] (for $Ш_{E/\mathbb{Q}}$).

References:

[1] Coates, J., Wiles, A.: On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. 39, 223-251 (1977)

[2] Gross, B., Zagier, D.: Heegner points and derivatives of L-series. Invent. Math. 84, 225-320 (1986)

[3] Kolyvagin, V.A.: Finiteness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a class of Weil curves. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. June 1988

[4] Kolyvagin, V.A.: On Mordell-Weil and Shafarevich-Tate groups of elliptic Weil curves. (Russian) preprint

[5] Milne, J.S.: Arithmetic duality theorems. Persp. in Math. 1, Orlando: Academic Press (1986)

[6] Rubin, K.: Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. Invent. Math. 89, 527-560 (1987)

[7] Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. 15, 259-331 (1972)

[8] Shimura, G.: Introduction to the arithmetic theory of automorphic forms. Pub. Math. Soc. Japan 11, Princeton: Princeton University Press (1971)

[9] Silverman, J.: The arithmetic of elliptic curves. Grad. Texts in Math. 106, New York: Springer (1986)

Title: *Abelian varieties and their division points*

Author: *Jean-Pierre SERRE*

Address: *Collège de France, 3 rue d'Ulm, 75005 Paris, France*

Lecture I.

Notation:

K finitely generated extension of $\mathbb{Q}$;

A abelian variety over K, of dimension $g > 0$;

ℓ prime number.

The Tate module $V_\ell A$ is defined as $\mathbb{Q}_\ell \otimes \varprojlim_{\alpha} A[\ell^\alpha]$, where $A[n]$ is the kernel of multiplication by n in $A(\overline{K})$. The Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ acts on $V_\ell A$; its image G_ℓ is an ℓ-adic Lie group, contained in $GL(V_\ell A) \equiv GL_{2g}(\mathbb{Q}_\ell)$. Its Lie algebra $\mathfrak{g}_\ell$ depends only on A, not of K.

The purpose of the lecture has been to state a number of known results on the structure of G_ℓ and $\mathfrak{g}_\ell$.

To state these, it is convenient to introduce the algebraic group H_ℓ = Zariski closure of G_ℓ. (Conjecturally, the connected component H_ℓ^o of H_ℓ should be the Mumford-Tate group M, over $\mathbb{Q}_\ell$; and there are many cases where this is known to be true, e.g. 5) below).

Results:

1) H_ℓ^o is a reductive group; G_ℓ is open in $H_\ell(\mathbb{Q}_\ell)$; the Lie algebra of H_ℓ is $\mathfrak{g}_\ell$.

2) The group $\mathbb{G}_m$ of homotheties is contained in H_ℓ.

3) Any $\mathbb{Q}_\ell$-endomorphism of $V_\ell A$ which commutes with H_ℓ^o (or $\mathfrak{g}_\ell$) belongs to $\mathbb{Q}_\ell \otimes \mathrm{End}_K A$.

4) The rank of H_ℓ^o is independent of ℓ.

(These results are due to Faltings, Bogomolov, Zarhin and others).

5) Assume a) $\mathrm{End}_{\overline{K}} A = \mathbb{Z}$.

b) g is odd, or $g = 2$ or $g = 6$.

Then H_ℓ is equal to $GSp_{2g}/\mathbb{Q}_\ell$, the group of symplectic similitudes, relative to the alternating form on $V_\ell A$ defined by a polarization of A.

In case 5), there is a more precise result (assuming K is a number field): the image of $G_K \to \prod_\ell GSp_{2g}(\mathbb{Q}_\ell)$ (adelic product) is *open*. In particular, the Galois group of the ℓ-division points of A is $GSp_{2g}(\mathbb{F}_\ell)$ for ℓ large enough. (In the case $g = 1$, i.e. A is an elliptic curve, this "large enough" can be made effective).

Note that the analogue of 5) for $g = 4$ would be false, as an example of Mumford shows.

References:

Résumé de cours au Collège de France, 1984-1985 (ℓ-adic)
Résumé de cours au Collège de France, 1985-1986 (variation with ℓ)

Lecture II.

To study the algebraic group $H_\ell = G_\ell^{alg}$ introduced in the first lecture, one makes use of the following information:

a) If v is a place of the ground field K (assumed to be a number field), with $v|\ell$, then the restriction of ρ_ℓ to the inertia subgroup I_v at v has a Hodge-Tate decomposition. From this follows that H_ℓ contains (after a suitable field extension) a "half-Hodge" torus, i.e. a multiplicative group G_m whose action on V_ℓ is $\begin{pmatrix} \mathbb{1}_g & 0 \\ 0 & \lambda\mathbb{1}_g \end{pmatrix}$ (where $\mathbb{1}_g$ is the unit matrix of size g).

b) Faltings' theorems tell us that H_ℓ^o is reductive, and that its commuting algebra is $\mathrm{End}_{\bar{K}} A \otimes \mathbb{Q}_\ell$.

c) If v is a place of K with good reduction, and $v \nmid \ell$, then the Tate module $V_\ell A$ can be identified with $V_\ell \tilde{A}_v$, where $\tilde{A}_v$ is the reduction of A at v. This identification is compatible with the action of the decomposition group D_v of v; the action of the inertia group I_v is trivial, and $D_v/I_v \cong \hat{\mathbb{Z}}$ acts via the Frobenius element π_v of $\tilde{A}_v$.

One thus gets an element $\pi_{v,\ell}$ of $G_\ell \subset H_\ell(\mathbb{Q}_\ell)$, which is well defined up to conjugation, and whose characteristic polynomial has coefficients in $\mathbb{Q}$, and is independent of ℓ. (Since the $\pi_{v,\ell}$ are dense in G_ℓ, this gives a strong relation between the ρ_ℓ's for various ℓ's). If $\Theta_{v,\ell}$ denotes the smallest algebraic subgroup of H_ℓ containing $\pi_{v,\ell}$, then $\Theta_{v,\ell}$ is obtained by scalar extension $\mathbb{Q} \to \mathbb{Q}_\ell$ from an algebraic group Θ_v of multiplicative type, defined over $\mathbb{Q}$, whose character group is the group generated by the eigenvalues of π_v. These Θ_v give precise information of H_ℓ. For instance, if H_ℓ is connected (which is true, e.g., if the 15-division points of A are rational over K), then $\Theta_{v,\ell}$ *is a maximal torus* of H_ℓ for a set of v of density 1 (this shows in particular that the rank of H_ℓ is independent of ℓ).

Using a), b), c) one can determine H_ℓ in various special cases, and prove in particular (cf. lecture I) that $H_\ell = GSp_{2g}/\mathbb{Q}_\ell$ if $\mathrm{End}_{\overline{K}} A = \mathbb{Z}$, and g is odd, 2 or 6.

Lecture III.

We study the variation of the Galois group with ℓ.

1) *The elliptic case.*

Let E be an elliptic curve over a number field K without complex multiplication, i.e. such that $\mathrm{End}_{\overline{K}} A = \mathbb{Z}$. It is known (Invent. Math., 1972) that there exists $L(E,K) > 0$ such that, for all $\ell > L(E,K)$, the Galois group $G(\ell)$ of the ℓ-division points of E is isomorphic to $GL_2(\mathbb{F}_\ell)$.

Thanks to the results of Faltings, the original proof can be much simplified (and it can also be made effective, cf. Sém. Th. des Nombres, Paris, 1988). But an even better simplification can be made, using the recent results of Masser-Wüstholz. One has to apply then to E and E × E, both on K and on a quadratic extension of K. More precisely one eliminates the Cartan subgroups and their normalizers according to the following pattern

	E	E × E
K	split Cartan	non split Cartan
K × K	normalizer of split Cartan	normalizer of non split Cartan

2) *Group-theoretic preliminaries for handling* $\dim A \geq 2$.

The main tool is a connection between subgroups of $GL_N(\mathbb{F}_\ell)$ and algebraic groups for N fixed, and ℓ large. By Jordan's theorem, a subgroup G of $GL_N(\mathbb{F}_\ell)$ whose order is prime to ℓ is "almost abelian", i.e. has an abelian normal subgroup C with $(G:C) \leq$ Jordan (N), where Jordan (N) is a constant depending only on N (e.g. Jordan $(2) = 60$). Hence, the main interest lies in subgroups G whose order is divisible by ℓ; let G^+ be the subgroup of G generated by its ℓ-Sylow groups. A construction due to Nori (Invent. Math. ~ 1986) attaches to G^+ an *algebraic subgroup* G^{+alg} of GL_N, namely the subgroup generated by all the one parameter subgroups $\{e^{tX}\}$, where X is a nilpotent matrix with $\exp(X) \in G^+$ (this makes sense if $\ell \geq N$). Nori proves that there is a constant $c(N)$ depending only on N such that the groups G^+ and $(G^{+alg}(\mathbb{F}_\ell))^+$ coincide, for $\ell > c(N)$. When G acts in a semi-simple way, G^{+alg} is a semi-simple algebraic group and $(G^{+alg}(\mathbb{F}_\ell))^+$ is the image of the rational points of the simply connected covering group of G^{+alg}.

This theorem allows us to use the standard methods of Lie theory almost as well as in the ℓ-adic case.

3) *Statement of results.*

(The notations A,K, ... are as before. I assume K is a number field, although the proofs should extend to extensions of finite type of $\mathbb{Q}$).

Theorem. *Let* $\rho : G_K \to \prod_\ell G_\ell$ *be the homomorphism defined by the surjective homomorphisms* $\rho_\ell : G_K \to G_\ell$. *If* K *is large enough, the image of* ρ *is open in* $\prod_\ell G_\ell$. *(i.e. the* ρ_ℓ*'s are almost independent).*

Theorem. *There is an exponent* $c \geq 1$ *such that* $\rho(G_K)$ *contains all homotheties in* $\hat{\mathbb{Z}}^* = \prod_\ell \mathbb{Z}_\ell^*$ *which are* c *powers.*

(It is likely that $\rho(G_K)$ contains a subgroup of finite index of $\hat{\mathbb{Z}}^*$, but I have not been able to prove it in general).

There are also several results of the "independence of ℓ" type. E.g. the rank of G_ℓ is independent of ℓ, and so is the finite group $(G_\ell^{alg}) / (G_\ell^{alg})^0$.

Assume now that A has no non trivial abelian subvariety of CM type. Then

a) *The set of places* v *of* A *where* $\tilde{A}_v$ *is supersingular has density* 0.

b) *If* x *is a torsion point of* A *of degree* d(x), *and of order* N(x), *one has*

$$d(x) >> N(x)^{2-\varepsilon} \qquad \textit{for every } \varepsilon > 0,$$

where the involved constant depends only on A,K,ε.

The proofs of these results have not been published, but a detailed exposition was given at the Collège de France in 1985/86; see also the "Résumé" in the Annuaire du Collège de France 1986/87, pp. 95-99.

Title: *Fiber systems of polarized abelian varieties*

Author: *Alice SILVERBERG*

Address: *Dept. Math., Ohio State University, 231 W. 18 Avenue,*
Columbus, Ohio 43210, U.S.A.

The subject of the talk was a conjecture and a theorem on the finiteness of Mordell-Weil groups of universal abelian varieties. One application of the main theorem is a new proof of Shioda's conjecture [2], first proved in [4], that the Mordell-Weil group of the universal principally polarized abelian variety (of dimension ≥ 2) with full level N (≥ 3) structure is exactly the group of N-torsion points. For details see [6], and for related results see [1-5].

We first introduce some notation. Suppose V is a real vector space of even dimension, E is a nondegenerate alternating bilinear form on V, and L is a lattice in V with $E(L, L) \subseteq \mathbb{Z}$. Suppose $I_0 \in GL(V)$, $I_0^2 = -1$, and $E(u, I_0 v)$ is symmetric and positive definite, and let K' be the centralizer of I_0 in the symplectic group Sp(V,E). Let G be a connected, semisimple real Lie group defined over $\mathbb{Q}$ and of hermitian type, let K be a maximal compact subgroup of G, and let ρ be a faithful representation of G in Sp(V,E), defined and irreducible over $\mathbb{Q}$, and preserving the Cartan decompositions. Let Γ be an arithmetic subgroup of G, without torsion, and with $\rho(\Gamma)L \subseteq L$. Let Δ be the complex manifold $\Gamma \backslash G / K$ and assume either $\dim \Delta > 1$ or Δ is compact. Letting $W = (\Gamma \ltimes L) \backslash (G/K \times V)$, a fiber space over Δ, it is possible to realize W as a complex manifold in such a way that the fiber over ΓgK is the abelian variety whose underlying complex torus is V / L with the complex structure $\rho(g)\, I_0\, \rho(g)^{-1}$, and with polarization given by E. The manifolds Δ and W can be realized as quasi-projective varieties. Let A be the generic fiber. Then A is an abelian variety defined over the function field $\mathbb{C}(\Delta)$. We can now state the conjecture.

Conjecture: $H^0(\Gamma,V) = 0 \Leftrightarrow A(\mathbb{C}(\Delta))$ is a finite group.

To state the theorem, we introduce two other fiber systems over Δ. Let $R = \Gamma \backslash (G/K \times V)$ and $Z = \Gamma \backslash (G/K \times L)$. Let S(W) (respectively S(R)) be the sheaf of germs of holomorphic sections of the fiber system $\overset{W}{\underset{\Delta}{\downarrow}}$ (respectively $\overset{R}{\underset{\Delta}{\downarrow}}$), and let S(Z) be the sheaf of germs of locally constant sections of $\overset{Z}{\underset{\Delta}{\downarrow}}$. We have an exact sequence $0 \to S(Z) \to S(R) \to S(W) \to 0$ of sheaves over Δ.

Consider the diagram:

$$\begin{tikzcd}
0 \arrow[r] & H^0(\Delta, S(Z)) \arrow[r] \arrow[d, "\cong"] & H^0(\Delta, S(R)) \arrow[r] & H^0(\Delta, S(W)) \arrow[r, "\delta"] & H^1(\Delta, S(Z)) \arrow[r] \arrow[d, "\beta"', "\cong"] & \dots & \\
0 \arrow[r] & H^0(\Gamma, L) \arrow[r] & H^0(\Gamma, V_{\mathbb{Q}}) \arrow[r] & H^0(\Gamma, V_{\mathbb{Q}}/L) \arrow[r] \arrow[u, hook, "f"'] & H^1(\Gamma, L) \arrow[r, "\alpha"] & H^1(\Gamma, V_{\mathbb{Q}}) \arrow[r] & \dots
\end{tikzcd}$$

where the vertical inclusion f, defined by $f(v + L)(\Gamma gK) = (\Gamma \ltimes L)(gK, v)$, defines an isomorphism from $H^0(\Gamma, V_{\mathbb{Q}}/L)$ onto $H^0(\Delta, S(W))_{\text{torsion}}$.

Theorem. $A(\mathbb{C}(\Delta))$ *is a finite group* $\Leftrightarrow H^0(\Gamma, V) = 0$ *and* $\alpha \circ \beta \circ \delta = 0$.

Corollary. $H^0(\Gamma, V) = 0$ *and* $H^1(\Gamma, V) = 0 \Rightarrow A(\mathbb{C}(\Delta))$ *is finite.*

The theorem follows from the lemmas below.

Lemma 1. $A(\mathbb{C}(\Delta)) \cong H^0(\Delta, S(W))$.

Lemma 2. $A(\mathbb{C}(\Delta))$ *is finitely generated* $\Leftrightarrow H^0(\Gamma, V) = 0$.

Lemma 3. $H^0(\Gamma, V) = 0 \Rightarrow H^0(\Delta, S(R)) = 0$.

References:

[1] G. van der Geer, K. Ueno: Nagoya Math. J. (1982)

[2] T. Shioda: On elliptic modular surfaces, J. Math. Soc. Japan 24(1972) 20-59

[3] A. Silverberg: Finiteness of Mordell-Weil groups of generic abelian varieties, Bull. AMS 12(1985) 131-133

[4] A. Silverberg: Mordell-Weil groups of generic abelian varieties, Invent. Math. 81(1985) 71-106

[5] A. Silverberg: Generic abelian varieties in the unitary case, to appear in Proc. AMS

[6] A. Silverberg: Cohomology of fiber systems and Mordell-Weil groups of abelian varieties, Duke Math. J. 56(1988) 41-46

Title: *Another proof of Mordell's conjecture over function fields (d'après P. Vojta)*

Author: *Christophe SOULÉ*

Address: *IHES, 35 route de Chartres, 91440 Bures-sur-Yvette, France*

Dyson's Lemma. *Let* C *be a projective curve of genus* g *over an algebraically closed field* k *of characteristic zero,* a,b ∈ C (k) *two rational points,* x (*resp.* y) *a local coordinate at* a (*resp.* b), L *a line bundle on* C × C, s *a holomorphic section of* L, *and* d_1, d_2 *two positive integers. In a neighbourhood of* ξ = (a,b) *write* s *as a power series*

$$s\ (x,y) = \sum_{\substack{i\geq 0\\ j\geq 0}} a_{ij}\, x^i y^j .$$

Definition. The index of s at ξ is

$$t\ (s,\xi,d_1,d_2) = \sup\ \{ t \mid i_1/d_1 + i_2/d_2 < t \Rightarrow a_{i_1 i_2} = 0 \} .$$

Theorem 1. *Let* $F_1 = x_0 \times C$ *and* $F_2 = C \times y_0$. *Choose* m *points* $\xi_1, \ldots, \xi_m$ *on* C × C. *Assume that*

i) $L.F_1 \leq d_1$, $L.F_2 \leq d_2$.

ii) s *does not vanish identically on a fiber of one of the projections from* C × C *to* C.

Let e *be the maximum multiplicity of a component in* div(s). *Then*

$$\frac{1}{2} \sum_{i=1}^{m} t^2\ (s,\xi_i,d_1,d_2) \leq \frac{L.L}{2d_1d_2} + \frac{e\ L.F_1}{2d_1d_2}\ \max(0,2g\text{-}2\text{+}m) .$$

To prove Theorem 1 one reduces to the case $d_1 = d_2$ by considering finite covers of C ramified at a (resp. b). When $d_1 = d_2$, the index is the multiplicity of the exceptional fiber of the blow up of C × C at ξ in the divisor of s (pulled back to this blow up).

Proof of Mordell's conjecture (sketch):

Let B be a smooth projective curve over k, F the function field of B, X → B a semi-stable curve and C = X ⊗ F; put g = genus (C).

Step 1: Assume $g \geq 2$. Let $p_1, p_2 : C \times C \to C$ be the two projections, ω the sheaf of differentials on C, and $r > 1$ a rational number. Let $\Delta \subset C \times C$ be the diagonal and define

$$\gamma = (g - \sqrt{g})/2 \qquad \delta = \gamma^2/(2g-2)^2\sqrt{g+1}$$
$$a_1 = \sqrt{(g+\delta)\,r} \qquad a_2 = \sqrt{(g+\delta)/r}\ .$$

Let

$$L = \mathcal{O}\left(\Delta + (a_1 - 1)\,p_1^*(\omega)/(2g-2) + (a_2 - 1)\,p_2^*(\omega)/(2g-2)\right).$$

Proposition 1. If $r > 2g(2g-2)/\delta$, L *is ample*. (Proof uses Nakai-Moishezon).

Step 2: Let $q : W = X \times_B X \to B$ and $V = q^{-1}(b_0)$ a fiber of q, $b \geq 0$, $d > 0$ integers, $\bar{\Delta}$ the closure of Δ, $\Omega = \omega_{X/B}$ the relative dualizing sheaf.

$$\mathcal{L} = \mathcal{O}\left(d\left(\bar{\Delta} + (a_1 - 1)\,p_1^*(\Omega)/(2g-2) + (a_2 - 1)\,p_2^*(\Omega)/(2g-2)\right)\right).$$

Proposition 2. *Let* r *be as in Proposition 1 and* $b > c_1\sqrt{r}/\delta$ *(where* c_1 *is a constant depending on* X*). Then, for* d *large enough,* $H^0(X, \mathcal{L}) \neq 0$. (Proof uses Riemann-Roch).

We shall apply Dyson's lemma to a section s of $\mathcal{L}$ with $d_1 = da_1$ and $d_2 = da_2$.

Step 3: According to Mumford there is a finite partition of $C(F)$,

$$C(F) = S_1 \amalg \ldots \amalg S_k$$

such that, if a,b lie in the same S_i, the corresponding points in the Jacobian of C (by the map $a \mapsto [a] - [\omega]/(2g-2)$) have a "bounded angle". In particular if E_1 (resp. E_2) is the closure of a (resp. b) in X, one gets a bound on $E_1 . E_2$, hence a bound on $E . \mathcal{L}$, where $E = p_1^*(E_1) . p_2^*(E_2)$ is a curve on W.

Step 4: Using the inequality from Step 3, the geometric construction describing the index (extended over B), and intersection theory on the appropriate blow up, one gets a *lower* bound for $t(s, \xi, da_1, da_2)$, when $\xi = (a,b)$, a and b lying in the same set S_i.

Step 5: Combining this lower bound with the *upper* bound coming from Dyson's lemma, one gets that, if the height h_1 of a is bigger than the height h_2 of b, there is an explicit constant c such that

$$h_2 < h_1 < c h_2\ .$$

Therefore each S_i is finite and $C(F)$ is finite. Furthermore, the number of elements in $C(F)$ can be explicitly bounded.

References:

P. Vojta: Dyson's lemma for products of two curves of arbitrary genus. Preprint, Berkeley 1988

P. Vojta: Mordell's Conjecture over Function Fields. Preprint, Berkeley 1988

Title: *p-adic Hodge theory for families of abelian varieties*

Author: *J.-P. WINTENBERGER*

Address: *Dept. Math., Université de Paris Sud, Bat 425, 91405 Orsay,*
France

Let p be a prime number. Let R be a domain with fraction field E of characteristic 0. Let $\bar{E}$ be an algebraic closure of E and $\bar{R}$ be the integral closure of R in $\bar{E}$. Let $\mathfrak{X}$ be an abelian scheme over R. Then one constructs a R[1/p]-algebra $B_{\bar{R}/R}$ and a natural isomorphism:

$$i : H^{*}_{DR}(\mathfrak{X}_{/R}) \underset{R}{\otimes} B_{\bar{R}/R} \cong H^{*}_{et}(\mathfrak{X}_{/\bar{E}}, \mathbb{Q}_p) \underset{\mathbb{Q}_p}{\otimes} B_{\bar{R}/R} .$$

The construction of $B_{\bar{R}/R}$ runs as Fontaine's construction of B_{DR} (B_{DR} = "B de Rham" is in case where R is a complete discrete valuation ring of characteristic (0,p) with perfect residue field). Given an integer $m \geq 1$ one shows there exists a R-algebra $\mathfrak{B}_m$ which is a p-adic infinitesimal thickening of the p-adic completion $\hat{\bar{R}}$ of $\bar{R}$ of order m, and which is universal for this property. Setting $B_m = \mathfrak{B}_m[1/p]$ and $B^{+}_{\bar{R}/R} = \varprojlim_{m} B_m$, one has an embedding of $T_p(G_m)(\bar{F})$ in $B^{+}_{\bar{R}/R}$ and if $t \in T_p(G_m)(\bar{F})$, $t \neq 0$, $B_{\bar{R}/R} = B^{+}_{\bar{R}/R}[1/t]$. The isomorphism i of the p-adic comparison theorem is defined using the universal vectorial extension $\mathcal{E}$ of $\mathfrak{X}$.

The powers of the kernel of $B^{+}_{\bar{R}/R} \rightarrow \hat{\bar{R}}[1/p]$ define a filtration on $B^{+}_{\bar{R}/R}$. If R [1/p] is smooth over a local field of mixed characteristic (0,p) with perfect residue field, the graduate ring of $B^{+}_{\bar{R}/R}$ is a formal series ring of d + 1 variables with coefficients in $\hat{\bar{R}}[1/p]$ (d = dimension of R [1/p]). If $S_\infty = \varinjlim_{i \in \mathbb{N}} gr^i(B^{+}_{\bar{R}/R})$ where $gr^i(B^{+}_{\bar{R}/R}) \rightarrow gr^{i+1}(B^{+}_{\bar{R}/R})$ is induced by multiplication by t, one has

$$H^{j}_{et}(\mathfrak{X}_{/\bar{E}}, \mathbb{Q}_p) \underset{\mathbb{Q}_p}{\otimes} S_\infty \cong \bigoplus_{i=0}^{i=j} H^{j-i}(X, \Omega^{i}_{X}) \underset{E}{\otimes} S_\infty(-i) .$$

When d = 0, one recovers Hodge-Tate decomposition. When $d \geq 1$, one recovers Hyodo "Hodge-Tate decomposition".

Furthermore, the Galois group $G = \mathrm{Gal}\,(\bar{E} / E)$ acts on $B_{\bar{R}/R}$ and under certain hypotheses on R one has $B^{G}_{\bar{R}/R} = \hat{R}\,[1/p]$. One constructs a derivation $B_{\bar{R}/R} \rightarrow B_{\bar{R}/R} \underset{R}{\otimes} \Omega^{1}_{R/O}$ and the isomorphism i is compatible with the Gauss-Manin connection (here one follows Faltings paper on Hodge-Tate decomposition for p-adic representations associated to modular forms).

Title: *Tate conjecture via transcendence*

Author: *Gisbert WUESTHOLZ*

Address: *ETH-Mathematik, Rämistrasse 101, 8092 Zürich, Switzerland*

We fix a number field K, an abelian variety A of dimension n defined over K and a prime number ℓ. We denote by π the Galois group Gal $(\bar{K}/K)$ and put

$$_{\ell^m}A := \mathrm{Ker}\,(A \xrightarrow{\ell^m} A)\,(\bar{\mathbb{Q}}),$$

$$T_\ell\,(A) := \varprojlim\, {}_{\ell^m}A\,.$$

A homomorphism $A^* \to A$ induces a homomorphism of Galois-modules

$$\mathrm{Hom}\,(A^*, A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}_\pi(T_\ell(A^*), T_\ell(A))\,.$$

Tate proved the injectivity of this homomorphism and conjectured its surjectivity. Furthermore he proved that his conjecture is implied by the following statement due to Lichtenbaum.

Hyp (K,A,d,ℓ): Given an abelian variety A of dimension n defined over a number field K, a prime ℓ and an integer $d \geq 1$ there exist only finitely many abelian varieties A^* over K such that

(i) there exists a polarization ψ of A^* of degree d^2 defined over K,

(ii) there exists a K-isogeny $\phi : A^* \to A$ with

$$\deg \phi = \ell^m, \text{ for some } m \geq 1.$$

This hypothesis was proved by G. Faltings in 1983. It is also implied by the following Theorem proved by D.W. Masser and the author.

Theorem. *There exists an effectively computable constant* $C > 0$ *depending only on the height* h(A) *of* A, dim A *and the degree of* K *over* $\mathbb{Q}$ *with the following property. If* A^* *is an abelian variety over* K *isogeneous to* A *over* K *then there exists an isogeny* $\phi : A^* \to A$ *over* K *with*

$$\deg \phi \leq C\,.$$

The proof goes as follows: Let ϕ be a minimal isogeny from A^* to A. Then ϕ induces a period relation and this can be used to define a homomorphism

$$\Psi : A^{2n} \rightarrow A^* .$$

The graph $\Gamma \subset A^{2n} \times A^*$ is an analytic subgroup. Now we apply transcendence technics and an effective version of the author's analytic subgroup theorem leads to an algebraic subgroup $H \subseteq \Gamma$. One then shows that $H = \Gamma$ and that the degree of H can be bounded by a constant as described in the theorem. Thus we can bound the degree of Γ. But now it is easy to get an isogeny from A to A^* using Γ of bounded degree and to bound finally the degree of ϕ.

Remark: Of course, this theorem gives another proof of the Mordell conjecture and again a proof of Siegels theorem using diophantine inequalities.