

## MATHEMATISCHES FORSCHUNGSIINSTITUT OBERWOLFACH

Tagungsbericht 34/1992

## Algebraische Zahlentheorie

2. bis 8. August 1992

Die Tagung fand unter der Leitung von Herrn Prof. G. Frey (Essen), Herrn Prof. H.-W. Leopoldt (Karlsruhe) und Herrn Prof. P. Roquette (Heidelberg) statt. Im Mittelpunkt des Interesses standen Probleme der klassischen Zahlentheorie. So wurde insbesondere berichtet über den aktuellen Stand der Forschung zu Fragen, die hauptsächlich aus der algebraischen und analytischen Zahlentheorie, aber auch aus der algebraischen und arithmetischen Geometrie und aus der konstruktiven und computerunterstützten Zahlentheorie stammen.

## Vortragsauszüge

## C.-G. SCHMIDT:

**Whittaker functions for twisted Rankin-Selberg convolutions on  $GL_n \times GL_{n-1}$** 

This talk reported on joint work with B. Mazur and D. Kazhdan where we study number theoretic properties of special (critical) values of  $L$ -functions  $L(\pi, \sigma, s)$  attached to pairs  $(\pi, \sigma)$  of cuspidal automorphic representations for  $GL_n$  resp.  $GL_{n-1}$  (at  $s = \frac{1}{2}$ ). A special case is the critical  $L$ -value  $L(E_1 \otimes \text{Sym}^2 E_2, 2)$  for modular elliptic curves  $E_i/\mathbb{Q}$ . We look for a uniform description of the twists  $L(\pi \otimes \chi, \sigma, \frac{1}{2})$  for all Dirichlet characters  $\chi$  of  $p$ -power conductor  $f$  (up to finitely many) for a fixed prime  $p$  where  $\pi$  and  $\sigma$  are unramified. Our main result is an integral formula for  $L(\pi \otimes \chi, \sigma, \frac{1}{2})$  which generalizes

from  $n = 2$  Birch's formula

$$G(\chi) \cdot L(f, \chi, 1) = \sum_{x \bmod f} \bar{\chi}(x) \int_{x/f}^{+\infty} f(z) dz$$

for the  $L$ -value of twisted new forms  $f \in S_2(\Gamma_0(N))$ . The main ingredient is the construction of a sensitive local Whittaker function  $w_\chi$  in the Whittaker module of  $\pi_p \otimes \chi$  such that the local zeta integral  $\Psi(w_\chi, v^0, s)$  is a certain non-vanishing constant for the new vector  $v^0$  in the Whittaker module of  $\sigma_p$ . For cohomological  $\pi$ ,  $\sigma$  this leads to rationality results.

## B. KÖCK:

### Das Adams-Riemann-Roch-Theorem in der höheren äquivarianten $K$ -Theorie

Ausgehend vom Riemann-Roch'schen Satz für Riemannsche Flächen wurde das äquivariante Riemann-Roch-Problem vorgestellt. Es lautet: Sei  $G$  eine (endliche) Gruppe und  $f : X \rightarrow Y$  ein eigentlicher Morphismus von  $G$ -Schemata. Man berechne die verallgemeinerte Euler-Charakteristik  $f_* : K_q(G, X) \rightarrow K_q(G, Y)$ . Dabei ist  $K_q(G, X)$  die  $q$ -te  $K$ -Gruppe zur Kategorie der  $G$ -Vektorbündel auf  $X$ .

Satz: Seien  $X$  und  $Y$  glatt. Ist  $f$  eine abgeschlossene Immersion oder operiert  $G$  auf  $X$  und  $Y$  trivial, so existiert und kommutiert das Adams-Riemann-Roch-Diagramm

$$\begin{array}{ccc} K(G, X) & \xrightarrow{\theta^*(T_f)^{-1}\psi} & K(G, X) \\ \downarrow f_* & & \downarrow f_* \\ K(G, Y) & \xrightarrow{\psi} & K(G, Y) \end{array}$$

Im zweiten Teil des Vortrages wurde die Konstruktion der  $\lambda$ -Struktur auf der höheren  $K$ -Theorie (das wesentliche Ingredient für die Grothendieck-Riemann-Roch-Theorie) nach Grayson erläutert. In diesem Zusammenhang konstruierten wir Shuffle-Produkte, die es ermöglichen zu zeigen, daß obige Äußere-Potenz-Operationen in erwarteter Weise mit den direkten Summen und den symmetrischen Potenzen zusammenhängen.

## A. WERNER:

### A proof of the Siegel/Mahler theorem using the Arakelov theory for arithmetical surfaces

Theorem (Siegel/Mahler): Let  $X_0$  be an affine curve of genus  $g \geq 1$  over a number field  $k$  and  $S$  a finite set of non-archimedean places of  $k$ . Then there are only finitely many  $S$ -integral points on  $X_0$ .

We sketched a proof of this theorem using Arakelov theory for arithmetical surfaces. This is for the Siegel version ( $S = \emptyset$ ) due to Faltings (in Cornell/Silverman: Arithmetic Geometry). Very roughly, this proof goes as follows: We may assume  $X_0 \subseteq X$ ,  $X$  projective, smooth curve; further there is an arithmetical surface prolonging  $X$ . For each  $P \in X(k)$  let  $D_P$  the closure of  $P$  in  $Z$  which is a horizontal Primdivisor. We may assume there is a point  $\infty \in X(k) \setminus X_0(k)$ ,  $m\infty$  is very ample for  $m \gg 0$  and

gives a projective embedding  $g$ . Then we can reduce the above theorem to Theorem 2: Let  $v$  be a place of  $k$ . For all  $C \in \mathbb{R}$ ,  $\varepsilon > 0$  the following inequality holds for almost all  $P \in X(k)$ :  $(D_P \cdot D_\infty)_v \leq C + \varepsilon [k : \mathbb{Q}] \lg(P)$ .

This is easy if we "stay away" with  $P$  from the point  $\infty$ . If not, we just get theorem 2 with  $\varepsilon > 2$  using the theorem of Roth. The general case follows by considering suitable étale coverings of  $X$ .

## F. HALTER-KOCH:

### Analytic number theory in algebraic function fields

(joint work with R. Warlimont)

Context: Abstract analytic number theory in formations (cf. J. Knopfmacher: Abstract Analytic Number Theory 1975, 1979).

Let  $D$  be a free abelian monoid with base  $P$ ,  $\partial : D \rightarrow \mathbb{N}_0$  s. t.  $(\partial(a) = 0 \Leftrightarrow a = 1)$ ,  $\partial(ab) = \partial(a) + \partial(b)$ ,  $\sim$  a congruence relation on  $D$  s. t.  $G = D/\sim$  is a finite group,  $N = \#G$ ,  $q > 1$ ;  $n = \gcd\{\partial a \mid a \in D, a \sim 1\}$ ,  $F : G \rightarrow \mathbb{Z}/n\mathbb{Z}$  s. t.  $F(g) = k + n\mathbb{Z} \Leftrightarrow \partial(a) \equiv k \pmod{n}$  for all  $a \in g$ . For  $g \in G$  set  $\gamma_g(k) = \#\{a \in g \mid \partial(a) = k\}$ ,  $\pi_g(k) = \#\{p \in P \cap g \mid \partial(p) = k\}$ ; clearly  $\gamma_g(k) = \pi_g(k) = 0$  if  $k \notin F(g)$ .

Axiom B. For  $k \in F(g)$ :  $\gamma_g(k) = Bq^k + O(s^k)$  ( $B > 0$ ,  $0 < s < q$ ).

Standard Example:  $K/\mathbb{F}_q$  algebraic function field,  $\emptyset \neq S$  finite set of places,  $R = \{f \in K \mid v(f) \geq 0\}$ ,  $\wp \triangleleft R$ ,  $D$  monoid of ideals rel. prime to  $\wp$ ,  $G$ : ray class group mod  $\wp$ .

Prime element theorem. Let Axiom B be satisfied,  $Z(z, \chi) = \sum_{g \in G} \chi(g) \sum_{a \in g} z^{\partial(a)}$  (for  $\chi \in G^* = \text{Hom}(G, \mathbb{C}^*)$ )

Case 1: The functions  $Z(z, \chi)$  do not have zeroes at  $|z| = q^{-1}$  at all. — Let  $q^{-1} < r < s^{-1}$  be s. t.  $Z(z, \chi)$  have no zeroes on  $|z| = r$ ,  $\max\{r^{-1}, \sqrt{q}\} \leq \xi < q$ ,  $g \in G$ . Then:  $[\text{For } k \in F(g) : \pi_g(k) = \frac{n}{N} \frac{q^k}{k} + O(\frac{s^k}{k})] \Leftrightarrow [\text{The } Z(z, \chi) \text{ do not have zeroes in } |z| < \xi^{-1}]$

Case 2: There are zeroes on  $|z| = q^{-1}$ . — Set  $\Delta = \ker(F) < G$ . Then there exists exactly one  $\varphi_0 \in \Delta^*$  s. t.  $Z(z, \chi)$  has a zero on  $|z| = q^{-1}$  iff  $\chi|\Delta = \varphi_0$ . We have  $\varphi_0^2 = 1$  and, setting  $v = -1$  resp.  $1$  if  $\varphi_0 = 1$  resp.  $\neq 1$  and  $G/\Delta = \langle \bar{g}_1 \rangle$  for a suitable  $g_1$ , if  $\chi|\Delta = \varphi$  then  $z = vq^{-1}\chi(g_1)^{-1}$  is a zero of  $Z(z, \chi)$ .

Prime element theorem: For  $k \in F(g) : \pi_g(k) = \frac{n}{N} \frac{q^k}{k} (1 - v^k \varphi_0(g_1^k g^{-1}) + O(\frac{s^k}{k}))$ , where  $\xi = \max\{r^{-1}, \sqrt{q}\}$ . Function fields: Case 1 with  $\xi = \sqrt{q}$ .

Conversions of the prime element theorem and Realization Theorems for semigroups in all cases are discussed.

## H.-G. RÜCK:

### Curves of genus 2

For an abelian variety  $A$  over a finite field  $\mathbb{F}_q$  let  $f_A(T)$  denote the characteristic polynomial of the Frobenius endomorphism;  $f_A(T)$  determines  $A$  up to isogeny. With the help of the Honda-Tate theorem one can produce the list of all occurring polynomials  $f_A(T)$ .

It is a natural question to ask which of these polynomials occur in the zeta function

of a curve over  $\mathbb{F}_q$ , i. e. which abelian varieties are isogenous to a Jacobian variety. For two-dimensional abelian varieties we give sufficient conditions on the coefficients of  $f_A(T)$  for the existence of such a curve.

In the second part we presented results of W. Kampkötter (thesis in Essen). Generalizing the classical ideas of the Weierstrass  $\sigma$ -,  $\wp$ - and  $\wp'$ -functions (following Mumford's lectures on theta) one gets explicit formulas for the Jacobian variety of curves of genus 2. This includes explicit addition formulas for the generalized Weierstrass functions and recursion formulas for  $n$ -division polynomials.

## K. MIYAKE:

### The Galois group of the second Hilbert $p$ -class field of a quadratic number field

Fix an odd prime  $p$ , and let  $k$  be a quadratic number field,  $\tilde{k}$  the Hilbert  $p$ -class field of  $k$  and  $\tilde{\tilde{k}}$  that of  $\tilde{k}$ , i. e. the second  $p$ -class field of  $k$ . Put  $G = \text{Gal}(\tilde{\tilde{k}}/k)$  and let  $G_1 = G \supset G_2 = [G_1, G] \supset G_3 = [G_2, G] \supset \dots$  be the lower central series of  $G$ . Hence  $G_1/G_2$  is isomorphic to the  $p$ -primary part  $C := \text{Cl}^{(p)}(k)$  of the ideal class group of  $k$ . We determine the structure of  $G_1/G_3$  by a theorem of Dr. Nomura in Osaka J. Math., 28 (1991), and analyze the structure of  $G_3$  by the capitulation problem for  $k$ . In particular, if  $k$  is an imaginary quadratic field, then we have

$$[G_1 : G_2] = |C|, [G_2 : G_3] = |C \wedge C|, |G_3| \geq |C \wedge C|^3$$

where  $C \wedge C$  is the alternating product of  $C$  by itself. We also have an estimate of the  $p$ -rank of  $G_3$ .

## B. W. MATZAT:

### Zopfgruppen und Einbettungsprobleme

In dem Vortrag wurde gezeigt, daß auch für mehrdimensionale GAR-Darstellungen der Einbettungssatz gilt: Sind  $K$  ( $= k(t_0)$ ) ein Hilberkörper und  $H$  eine endliche Gruppe, deren Kompositionsfaktoren GAR-Darstellungen über  $K$  besitzen, so besitzt jedes endliche (reguläre) Einbettungsproblem über  $K$  eine (reguläre) Lösung (für den 1-dimensionalen Fall siehe Konstruktive Galoistheorie, Kap. IV).

Daran anschließend wurde gezeigt, wie sich die Automorphismenbedingung  $A$  und die Rationalitätsbedingung  $R$  einer GAR-Darstellung im mehrdimensionalen Fall nachweisen lassen. Mit dem vorgeführten Beispiel  $L_3(4)$  und weiterer neuer Resultate des Vortragenden sowie von Häfner, Malle und Völklein konnte damit u. a. die Liste der GAR-Darstellungen einfacher Gruppen  $G$  über  $\mathbb{Q}$  mit  $|G| < 29120$  vervollständigt werden bis auf die Gruppen  $L_2(q)$  mit  $q = 9, 25, 27$  (siehe Manuscripta Math. 74, 217 - 222 (1992)).

## K. WINGBERG:

### Unverzweigte Erweiterungen algebraischer Zahlkörper

Folgende Sätze wurden vorgestellt: Sei  $p$  eine Primzahl.

**Satz 1:** Sei  $k = \mathbb{Q}(\zeta_p)$  und sei die Vandiver-Vermutung für  $p$  richtig, d. h.  $p$  teilt nicht die Klassenzahl  $h^+$  von  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ . Dann ist der  $p$ -Klassenkörperturm von  $k$  unendlich, falls der Rang  $d$  der Klassengruppe von  $k$  größer oder gleich 3 ist.

**Satz 2:** Sei  $L$  die maximale unverzweigte  $p$ -Erweiterung der zyklotomischen  $\mathbb{Z}_p$ -Erweiterung  $k_\infty$  von  $k = \mathbb{Q}(\zeta_p)$ . Dann gilt:  $\text{Gal}(L/k_\infty)$  ist eine endlich erzeugte freie pro- $p$ -Gruppe genau dann, wenn  $p \nmid h^+$  gilt.

**Bemerkungen:** Ist  $d = 2$ , so ist unter einer Zusatzvoraussetzung auch in diesem Fall der  $p$ -Klassenkörperturm von  $k$  unendlich. Insbesondere ist  $\mathbb{Q}(\zeta_{157})$  der kleinste Körper der Form  $\mathbb{Q}(\zeta_p)$ ,  $p$  Primzahl, mit unendlichem  $p$ -Klassenkörperturm. Beide Sätze gelten allgemeiner für algebraische Zahlkörper vom CM-Typ, die  $\zeta_p$  enthalten und für die die Iwasawa-Vermutung  $\mu = 0$  richtig ist. Der Beweis von Satz 1 folgt leicht aus Satz 2 unter Benutzung der Formel von Goloch und Shafarevich. Es zeigt sich nämlich, daß die Galoisgruppe  $\text{Gal}(L_0/k)$  der maximalen unverzweigten  $p$ -Erweiterung  $L_0$  von  $k$  eine Schurgruppe ist, d. h. genauso viele Erzeugende wie definierende Relationen besitzt. Der Beweis von Satz 2 benutzt nicht-abelsche Methoden, d. h. das Konzept der pro- $p$ -Operatorgruppen.

## A. SCHMIDT:

### Fundamentalgruppen glatter arithmetischer Flächen

Folgende Sätze, die aus einer Zusammenarbeit mit K. Wingberg entspringen, wurden vorgestellt:

**Satz 1:** Sei  $K$  ein lokaler Körper,  $l$  eine Primzahl  $\neq \text{char } K$ ,  $X/K$  eine glatte proj. Kurve vom Geschlecht  $g \geq 1$ . Nehmen wir an, daß die  $l$ -Torsionspunkte der Jacobischen von  $X$  rational über  $K$  liegen, so ist der maximale pro- $l$ -Faktor  $\pi_1^{\text{et}}(X/K)(l)$  der étalen Fundamentalgruppe eine Poincare-Gruppe der Dimension 4 mit dualisierendem Modul  $\mathbb{Q}_l/\mathbb{Z}_l(2)$ .

**Bemerkung:** Satz 1 gilt entsprechend auch für Kurven über  $n$ -dimensionalen lokalen Körpern.

**Satz 2:** Sei  $K$  ein globaler Körper,  $l \neq \text{char}(K)$  eine Primzahl und  $X_K$  eine geometrisch zusammenhängende, glatte und eigentliche Kurve über  $K$  vom Geschlecht  $\geq 1$ , die einen  $K$ -rationalen Punkt besitzt. Wir nehmen an, daß die  $l$ -Torsionspunkte der Jacobischen rational liegen. Sei  $S$  eine endliche Stellenmenge von  $K$ , die mindestens zwei Stellen enthält und im Zahlkörperfall  $S \supset S_l \cup S_\infty$ . Im Zahlkörperfall nehmen wir noch an, daß  $K/\mathbb{Q}$  Galoisch,  $\#S_l(K) > 1$  und für  $l = 2$  sei  $K$  total imaginär. Sei nun  $\mathcal{X}_{\mathcal{O}_S}$  ein glattes und eigentliches Modell von  $X$  über  $\text{Spec}(\mathcal{O}_S)$ . Dann ist  $\pi_1^{\text{et}}(\mathcal{X}_{\mathcal{O}_S})(l)$  eine Dualitätsgruppe der Dimension 4 mit dualisierendem Modul  $\text{Tor}_l - C_S(K)(1)$ , d. h. für alle  $i \geq 0$  und jeden endlichen  $l$ -primären  $\pi_1(X)(l)$ -Modul  $M$  induziert das Cup-Produkt

$$\cup : H^i(\pi_1(\mathcal{X})(l), M) \times H^{4-i}(\pi_1(\mathcal{X})(l), \text{Hom}(M, \text{Tor}_l - C_S(K)(1))) \\ \rightarrow H^4(\pi_1(\mathcal{X})(l), \text{Tor}_l - C_S(K)(1)) \xrightarrow{\text{tr}} \mathbb{Q}_l / \mathbb{Z}_l$$

eine perfekte Paarung enldicher abelscher Gruppen.

## M. FLACH:

### Deformation von Galoisdarstellungen

Thema des Vortrags war der Beweis eines Spezialfalles einer Vermutung von Mazur und Tilouine: Sei  $R$  eine lokale, ordinäre Komponente der von Hida definierten  $p$ -adischen Hecke-Algebra für  $GL_2/\mathbb{Q}$  mit Führer  $N$  prim zu  $p$ . Dann existiert eine Darstellung  $\rho_R : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(R)$  und alle im üblichen Sinne zu  $p$ -ordinären Spitzenformen vom Führer  $Np^r$  assoziierten Galoisdarstellungen faktorisieren über ein solches  $\rho_R$ . Sei andererseits  $R^0$  der universelle ordinäre Deformationsring der zu  $\rho_R$  assoziierten Restklassendarstellung  $\bar{\rho}_R : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(k)$  ( $R$  ist lokal, noethersch, vollständig mit Restklassenkörper  $k$ ,  $[k : \mathbb{F}_p] < \infty$ ). Unter geeigneten Bedingungen an  $\bar{\rho}_R$  existiert  $R^0$  zusammen mit einer Darstellung  $\rho_{R^0} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(R^0)$ , über die alle Lifts von  $\bar{\rho}_R$  nach  $GL_2(A)$ ,  $A$  lokal, noethersch, vollst. mit Restklassenkörper  $k$ , faktorisieren. Also gibt es einen Morphismus  $\varphi : R^0 \rightarrow R$ . Nach einem Resultat von Mazur-Tilouine-Gouven ist dieser  $\Lambda$ -linear und surjektiv für eine natürliche  $\Lambda$ -Algebra-Struktur auf beiden Ringen ( $\Lambda = \mathbb{Z}_p[[T]]$ ). Die Vermutung von Mazur-Tilouine ist, daß  $\varphi$  ein Isomorphismus ist. Dies kann gezeigt werden für lokale Komponenten  $R$ , die zu modularen elliptischen Kurven gehören und für die  $p \nmid L(\text{Sym}^2 E, 2) \cdot \Omega^{-1}$  (im wesentlichen). Letztere Bedingung erzwingt sogar  $R^0 = \Lambda$ . Die Beweismethode basiert auf Ideen von Kolyvagin unter Ausnutzung der Geometrie von Modulkurven und  $K$ -Theorie. In Arbeit ist eine Verallgemeinerung auf andere lokale Komponenten  $R$ . Es besteht Hoffnung auf eine Elimination der Bedingung  $p \nmid L$ -Wert, d. h. einen völlig allgemeinen Beweis der Vermutung.

## T. METSÄNKYLÄ:

### Cyclotomic invariants up to one million

Since the computational work by Wagstaff (1978) and his predecessors, one knows the values of certain cyclotomic invariants, notably the Iwasawa invariants  $\lambda_p$  and  $\nu_p$ , for all primes  $p < 125,000$ . In 1987, Tanner and Wagstaff extended parts of these computations to 150,000, and recently Buhler, Crandall and Sompolski went on, with a new method, up to  $10^6$ . In a joint work with Ernwall, I have completed the computations to include the missing information about  $\lambda_p$  and  $\nu_p$ . Some new techniques had to be developed. In the results there appear no new phenomena.

## H. COHN:

### Projection of quadratic forms from fields to subfields

Let  $k_0 = \mathbb{Q}(\sqrt{D})$ ,  $D$  square-free  $> 1$ , discriminant  $\sigma^2 D$ , ( $\sigma \in \{1, 2\}$ ), and integer ring  $\mathcal{O}_0$ . Let  $A > 0$  be an integer with only one odd prime divisor (at most). Then if

$p = \pi\pi'$  in  $\mathcal{O}_0$ , we have a "projection" from  $k_0$  to  $\mathbb{Q}$ :

$$(*) \quad \{\pi = \xi^2 + A\eta^2\} \Rightarrow \{p = x^2 + Ao^2y^2 = u^2 + ADo^2v^2\}.$$

This is easily proved by factoring  $p$  in  $\mathbb{Q}(\sqrt{D}, \sqrt{-A})$ . Conjecturally the converse of " $\Rightarrow$ " is valid (producing " $\Leftrightarrow$ ") if and only if  $\text{Class\#}(k_0) = 1$ . In terms of Ring Class Fields (over  $\mathbb{Q}$ ),  $(*)$  means:

$$(**) \quad \text{RCF}(\xi^2 + A\eta^2) \geq \text{RCF}(x^2 + Ao^2y^2) \times \text{RCF}(u^2 + ADo^2v^2).$$

Now  $(**)$  can be changed from " $\geq$ " to " $=$ " by verifying equal degrees. The result  $(*)$  or  $(**)$  has been verified for  $A = 2^t$ ,  $t \geq 0$ , (all  $D$ ) and for  $D = 2$ , (all  $A$ ) (see Proc Num Theory Conf Kingston 1991).

Remarks: (1) The converse of "projection" ( $\Rightarrow$ ) or "lifting" ( $\Leftarrow$ ) establishes relations between  $2^n\|N(\eta)$  and  $2^g\|(y, v)$ . The simplest is for  $D = 2$ :  $\pi = \xi^2 + 2^t\eta^2 \Leftrightarrow p = x^2 + 2^{t+1}y^2 = u^2 + 2^{t+2}v^2$ .

(2) The process can work for other base fields (not only  $\mathbb{Q}$ ). In Crelle 361 (1985) it is applied to the tower  $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2+\sqrt{2}}) \subset \mathbb{Q}(\sqrt{2+\sqrt{2+\sqrt{2}}})$ .

(3) The reduction  $(*)$  is equivalent in principle to the use of diagonals of the fundamental domain for Hilbert Modular Functions (see Math. Ann. 265 (1983)).

## E. BAYER-FLUCKIGER:

### Lattices and number fields

(joint work with J. Martinet)

Let  $K_1, \dots, K_r$  be totally real number fields, and  $K_{r+1}, \dots, K_s$  be totally imaginary number fields with involutions  $\bar{\phantom{x}} : K_i \rightarrow K_i$  such that  $F_i := \{x \in K_i \mid \bar{x} = x\}$  is totally real. Set  $K = K_1 \times \dots \times K_s$ , and let  $\bar{\phantom{x}} : K \rightarrow K$  be the induced involution. Let  $F = \{x \in K \mid \bar{x} = x\}$ , and let  $a \in F$  be totally positive. Then  $S : K \times K \rightarrow \mathbb{Q}$ , defined by  $S(x, y) = \text{Tr}_{K/\mathbb{Q}}(ax\bar{y})$ , is a positive definite symmetric bilinear form. Let  $\mathcal{O}$  be an order of  $K$ , and let  $\delta = \{x \in K \mid \text{Tr}(x\vartheta) \subseteq \mathbb{Z}\}$ . Let  $I$  be an  $\mathcal{O}$ -ideal. Then  $(I, S)$  is said to be an  $\mathcal{O}$ -lattice if and only if  $aI\bar{I} \subseteq \delta$ , in other words, if  $S(x, y) \in \mathbb{Z}$  for all  $x, y \in I$ .

This talk presented some properties of  $\mathcal{O}$ -lattices especially in the case where  $K$  is a totally imaginary field. It also contained several examples: for instance, the Coxeter-Todd lattice is an  $\mathcal{O}$ -lattice for  $\mathcal{O} = \mathbb{Z}[\zeta_{21}]$ , the Leech lattice for  $\mathcal{O} = \mathbb{Z}[\zeta_{35}]$ .

## N. KLINGEN:

### Weak decomposition laws of number fields

By definition the weak Kronecker equivalence (KE) of number fields  $K, K'/k$  over  $k$  means that their Kronecker sets  $D(K/k)$ ,  $D(K'/k)$  are equal up to at most finitely many exceptions. Here  $D(K/k)$  is the set of primes  $\rho \in P(k)$  having in  $K$  a prime factor  $\mathfrak{P}$  of residue degree  $f(\mathfrak{P}/\rho) = 1$ . With  $f_1 \leq \dots \leq f_r$  denoting all residue degrees of  $\rho$  in  $K$  the stronger arithmetical equivalence (AE) of  $K, K'$  over  $k$  states that for almost all primes  $\rho \in P(k)$  the residue degrees are all the same:  $f_i = f'_i$ . Though the condition for (KE) seems that weak there are many results proving  $(\text{KE}) \Rightarrow (\text{AE})$ .

Now, in a thesis at Köln (1992) M. Lochter obtained new characterizations of (KE) with arithmetic consequences (mainly for various norm groups). One result is as follows:

Theorem:  $K, K' \text{ (KE)} \Leftrightarrow f_1 = f'_1 \text{ for all } \rho \Leftrightarrow \mathbb{N}f_1 + \dots + \mathbb{N}f_r = \mathbb{N}f'_1 + \dots + \mathbb{N}f'_r \text{ for all } \rho$ . ( $f_i$  denotes the smallest residue degree.)

The ramified primes  $\rho$  are included! The last statement about the coincidence of the semigroups generated by  $f_1, \dots, f_r$ , gives the link to norm groups and a characterization of (KE) over  $\mathbb{Q}$  in terms of the zeta function.

## R. ODONI:

### Simple proof that $L(1, \chi) \neq 0$ for ray-class characters

Let  $K$  be an alg. number field and let  $\chi$  be a ray-class character  $(\text{mod } *f)$  of  $K$ ,  $f$  some cycle. The result that  $L(1, \chi) \neq 0$  for  $\chi \neq \chi_0$  is crucial for the proof that every ray-class  $(\text{mod } *f)$  contains infinitely many prime ideals (indeed, that prime ideals are equidistributed amongst the ray-classes). Classically, the proof of  $L(1, \chi) \neq 0$  depends either on a continuation of  $L(s, \chi)$  into  $\text{Re } s > 0$  (Hecke) or even on the main theorems of classfield theory. We give a simple proof using only a continuation into  $\text{Re } s > 1 - [K : \mathbb{Q}]^{-1}$  (Weber) and the simple proof (Siegel) of the quadratic reciprocity law in  $K$ .

## W. D. GEYER:

### Das letzte Lemma von Eisenstein

Wenige Monate vor seinem Tod (1852) mit 29 Jahren publizierte Eisenstein eine kurze Note, in der er feststellte, daß für jede algebraische Potenzreihe  $f(t)$  mit  $f'(0) \neq 0$  über  $\mathbb{Q}(t)$  eine natürliche Zahl  $m$  existiert, so daß  $f(mt)$ , abgesehen vom 0-ten Koeffizienten, eine Potenzreihe mit ganzen Koeffizienten ist. Präziser lassen sich die Beträge der Koeffizienten einer Potenzreihe  $f(t)$  mit  $F(f(t), t) = 0$ ,  $f(0) = \alpha$ ,  $\frac{\partial F}{\partial x}(\alpha, 0) = \beta \neq 0$  sehr gut durch die Beträge der Koeffizienten von  $F$ ,  $\alpha$  und  $\beta$  abschätzen — solange der Betrag nichtarchimedisch ist. Im klassischen archimedischen Fall ist die Sachlage etwas diffiziler. Bombieri in seiner Arbeit zur Mordellschen Vermutung (Pisa 1991) gibt für  $|\alpha| \leq 1$  eine Abschätzung  $|c_n| \leq (2 \cdot \deg F)^{5n} \cdot (\frac{|F|}{|\beta|})^{2n-1}$  für den  $n$ -ten Koeffizienten  $c_n$  von  $f(t)$ , deren Beweis nicht ganz stichhaltig ist, sondern nur  $|c_n| \leq (2 \cdot \deg F)^{7n} \cdot (\frac{|F|}{|\beta|})^{2n-1}$  für  $n \geq 1$  liefert. Hier wird eine Abschätzung  $|c_n| \leq D^n \cdot \max(1, \frac{|F|}{|\beta|})^{2n-1}$  gezeigt mit  $D = d^4(d+6)$ , wo  $d = \deg_x F$  ist. Die numerischen Experimente für  $d \leq 100$  zeigen, daß man mit  $D = d^4$  für  $d > 2$  auskommen sollte.

## E.-W. ZINK:

### Vergleich der Darstellungen von $GL_N$ und Divisionsalgebren über einem lokalen Körper

Es wurde ein System von Parametern eingeführt, welches in nichtkanonischer Weise sowohl den quadratisch integrierbaren irreduziblen Darstellungen von  $GL_N(F)$  als auch

den sämtlichen irreduziblen Darstellungen von  $D^\times$  (= multiplikative Gruppe einer zentralen Divisionsalgebra vom Index  $N$  über  $F$ ) entspricht. Daraus ergeben sich Bijektionen zwischen den genannten Mengen von Darstellungen, welche verträglich sind mit zahmem Charaktertwist, den Artin-Führer invariant lassen und die Eigenschaft haben, daß der formale Grad einer quadratisch integrierbaren Darstellung von  $GL_N(F)$  gleich ist der Dimension der dazu korrespondierenden Darstellung von  $D^\times$ . Die Parameter sind sogenannte  $R$ -Polynome, d. h. Galoisorbits von Paaren  $(R, \beta)$ , wobei  $\beta \in \bar{F}$  algebraisch ist über  $F$  und  $R$  eine irreduzible Darstellung der zahmen Galoisgruppe  $\text{Gal}(\bar{F}(\beta)/F(\beta))$  ( $\bar{F}/F$  bezeichnet die maximale zahme Erweiterung in dem algebraischen Abschluß  $\bar{F}$ ). Die Menge  $T_N^-$  aller  $R$ -Polynome mit der Eigenschaft, daß  $\dim(R) \cdot [F(\beta) : F]$  ein Teiler von  $N$  ist und daß das Minimalpolynom  $f_\beta(T)$  über  $F$  ein "Minuspolygon" ist, ergibt das eingangs erwähnte Parametersystem.

### J. RITTER:

#### On the Galois structure of $S$ -units

The talk which reports on joint work with A. Weiss is about the  $G$ -structure of  $S$ -units  $E$  in an absolutely abelian number field  $N$  of odd degree with Galois group  $G$ . We first change the so-called Tate sequence for  $E$ , by which the cohomology of  $E$  is given, into one for  $U = E/\text{tor}(E)$ , which then is of type  $0 \rightarrow U \rightarrow P \rightarrow F \rightarrow H \rightarrow 0$ , where  $P$  is projective,  $F$  free and where  $H$  is the Dirichlet lattice defined by  $0 \rightarrow H \rightarrow \bigoplus_{v \in S} \mathbb{Z} v \xrightarrow{v^{-1}} \mathbb{Z} \rightarrow 0$ . The existence of the Tate sequence for  $E$  requires the finite set  $S$  of primes of  $N$  to be rather big: namely,  $S \supset \{\infty, \text{ramified primes}\}$  and  $h_S = 1$ ;  $S$  is also supposed to contain at least one completely split prime. Form the above sequence for  $U$  one can derive a new sequence  $0 \rightarrow Y \rightarrow F \rightarrow F \rightarrow H \rightarrow 0$  by which  $Y$  is uniquely defined (independent of  $F$  and the special map); moreover,  $Y$  and  $U$  belong to the same genus. Then, by means of the Fröhlich regulator, the deviation of  $U$  from  $Y$  is measured. It turns out that a theorem of Fröhlich (Crelle 1989) on the leading coefficient  $c(\chi)$  of the Taylor series at  $s = 0$  of the Artin  $L$ -function  $L(s, \chi)$  (with the Euler factors of primes in  $S$  removed) can be exploited in order to obtain:

$$\chi \mapsto |G| - \text{prime part of } R(\bar{\chi}, g)/c(\bar{\chi})$$

is a representing Galois homomorphism for  $U - Y$  in the genus class group of  $Y$ . Here,  $\chi$  runs through the irreducible characters of  $G$  and  $R(\bar{\chi}, g)$  is the Stark regulator of the contragredient character  $\bar{\chi}$  and a "genus" map  $g : Y \hookrightarrow U$  the cokernel of which is prime to  $|G|$ . Also, a module theoretic interpretation of the Chinberg invariant which comes from the Tate sequence is given.

### M. TAYLOR:

#### Galois module structure and Mordell-Weil groups

Let  $G$  be a finite abelian group and let  $K$  be a number field. We then consider a Hopf order  $\mathcal{A}$  in  $KG$  and its Cartier dual  $\mathcal{B}$  in  $B = \text{Map}(G, K)$ . The main aim of the lecture was to consider the "class" map  $\psi_B$  from  $\text{PH}(\mathcal{B})$ , the group of principal

homogeneous spaces of  $\mathcal{B}$ , to  $\text{Cl}(\mathcal{A})$ , the classgroup of locally free  $\mathcal{A}$ -modules. This set-up was studied in detail in two situations:

(a) When  $|G| = p$ , prime, where the Tate-Oort classification can be used to determine all  $\mathcal{B}$  (for given  $K$ ). In particular, when  $\mathcal{B} = \text{Map}(G, \mathcal{O}_K)$ , then it was shown that the size  $\text{Ker}(\psi_{\mathcal{B}})$  was determined by  $p$ -adic  $L$ -function congruences.

(b) The most interesting case occurs when  $\mathcal{B}$  comes from the group scheme of points of (a given) finite order; then  $\psi$  can be received as defining a class map on the Mordell-Weil group. Under suitable circumstances  $\text{Ker}(\psi)$  always contains the torsion points, and that a point of infinite order can be divided by a sufficiently large power of a given endomorphism so as to produce a non-trivial class.

## G. R. EVEREST:

### On the proximity of algebraic units to divisors

Let  $K/\mathbb{Q}$  denote a finite, totally real extension, with  $U_K$  denoting the group of units of the ring of algebraic integers. Suppose  $p$  is a prime of  $\mathbb{Q}$  which splits totally in  $K$ . Then  $\sigma_1, \dots, \sigma_{r+1} : K \rightarrow \mathbb{R}$  ( $r+1 = [K : \mathbb{Q}]$ ) are distinct embeddings, as are  $\tau_1, \dots, \tau_{r+1} : K \rightarrow \mathbb{Q}_p$ . Define  $\lambda_{D,\infty}(u) = \max_{1 \leq i \leq r+1} \log |\sigma_i(u)|$ ,  $\lambda_{D,p}(u) = \max_{1 \leq i \leq m} \log |\tau_i(u) - 1|_p$  for  $1 \leq m \leq r+1$ . (The presence of  $D$  indicates that these are Weil functions for a divisor on a variety containing  $U_K$ ). Let  $N_{D,S}(u) = \lambda_{D,\infty}(u) + \lambda_{D,p}(u)$  ( $S = \{\infty, p\}$ ) a proximity function.

Theorem: Let  $G < U_1$  (the 1-units) of finite index. There exist constants  $A_K > 0$  and  $\theta_{D,G}$  with the property  $\#\{u \in U_K : N_{D,S}(u) < Q\} = A_K Q^r + r A_K \theta_{D,G} \log p \theta^{r-1} + o(Q^{r-1})$  as  $Q \rightarrow \infty$ , provided  $1 < m$ . Moreover  $\theta_{D,G} \in \mathbb{Q}$ .

The expression  $\theta_{D,G} \log p$  represents the average  $p$ -adic proximity of  $U_K$  to the divisor  $D$ . Two special cases were presented in the talk, of calculations of  $\theta_{D,G}$  — showing that it gives a very agreeable  $p$ -adic geometric interpretation of the embedding of the global units in  $p$ -adic space. Also, a consideration was given to the conjecture that  $\theta_{D,G}$  exists if  $m = 1$ . In this circumstance the average proximity is of a surprising kind, involving a transcendental invariant of  $K$ .

## E. KLEINERT:

### Einheiten klassischer Ordnungen (Übersicht)

Der Vortrag gab eine Übersicht über die wichtigsten bekannten Resultate über Einheiten von Ordnungen endlich-dimensionaler, halbeinfacher  $\mathbb{Q}$ -Algebren. Themen waren: (1) elementare Eigenschaften (2) endliche Erzeugung (klassische Reduktionstheorie) (3) Präsentationen I: die Theorie der Transformationsgruppen (4) Präsentationen II: indefinite Quaternionenschiefkörper über  $\mathbb{Q}$  (5) Präsentationen III:  $K_2$  (6) Kohomologie (7) Kongruenzgruppen und Normalteiler (8) der Einheitensatz von Bass (9) auf der Suche nach einem allgemeinen Einheitensatz (Aus Zeitgründen kamen (6) – (8) nicht im Vortrag vor).

## C. DENINGER:

### Evidence for a cohomological approach to analytic number theory

Let  $k$  be a number field,  $\wp$  a prime of  $k$ . To any mixed motive  $M$  over  $k_\wp$  one can associate an  $L$ -factor  $L_\wp(M, s)$ . Setting  $\mathbb{L}_\wp = \mathbb{C}[\exp(\frac{2\pi i}{\log N_\wp} \xi), \exp(-\frac{2\pi i}{\log N_\wp} \xi)]$  if  $\wp \neq \infty$  and  $\mathbb{L}_\wp = \mathbb{C}[\exp(-[C : k_\wp] \xi)]$  if  $\wp = \infty$  we have proved:

**Theorem:** There exist additive functors

$$\mathcal{F}_\wp : \{\text{mixed motives over } k_\wp\} \rightarrow \{\mathbb{L}_\wp[\frac{d}{d\xi}] \text{-modules, free over } \mathbb{L}_\wp \text{ of finite rank}\}$$

such that  $\text{rk}_{\mathbb{L}_\wp} \mathcal{F}_\wp(M) = \begin{cases} \dim_{k_\wp} M^I_\wp & \text{if } \wp \neq \infty \\ \dim_{k_\wp} M_S & \text{if } \wp = \infty \end{cases}$  and  $H^*(X/\mathbb{L}_\wp) := \mathcal{F}_\wp(H^w(X))$ . defines a cohomology theory on good reduction varieties  $X/k_\wp$  and such that  $L_\wp(M, s) = \det_\infty(\frac{1}{2s}(s - \theta) | \mathcal{F}_\wp(M))^{-1}$ , where  $\theta = \frac{d}{d\xi}$  and  $\det_\infty$  is the zeta-regularized determinant. For a site containing  $\overline{\text{Spec } \mathcal{O}_k}$  with specified properties (in particular  $\mathcal{F}_\wp(M) = \mathcal{F}(M)_\wp$  for a sheaf  $\mathcal{F}(M)$  over  $\overline{\text{Spec } \mathcal{O}_k}$ ) a Lefschetz trace formula would read as follows:

$$\sum_{i=0}^2 (-1)^i \text{Tr}(\Phi(\theta) | H^i(\overline{\text{Spec } \mathcal{O}_k}, \mathcal{F}(M))) = \sum_{\wp} \text{Tr}(\Phi(\theta) | \mathcal{F}_\wp(M)),$$

for suitable analytic functions  $\Phi$ . We discussed a consequence of this formula that can be proved and which gives a reinterpretation of the explicit formuals in analytic number theory as a fixed point formula. Finally we sketched a simple “proof” of the Riemann hypothesis for  $\zeta_k(s)$ , using the above hypothetical formulism.

## E. NART:

### Motive über arithmetischen Kurven

Sei  $X = \overline{\text{Spec } \mathcal{O}_K}$  die arithmetische Kurve im (naiven) Sinne von Arakelov, zum Ring  $\mathcal{O}_K$  der ganzen Zahlen eines Zahlkörpers  $K$  assoziiert. Die Kategorie  $\mathcal{MM}_X$  von gemischten Motiven über  $X$  ist definiert als die Unterkategorie von  $\mathcal{MM}_K$  (gemischte Motive über  $K$ ) der Motive, die an allen Primstellen eine gewisse “Ganzheits”-Bedingung erfüllen. Man definiert einen Spurhomomorphismus  $\text{Ext}_{\mathcal{MM}_X}^2(\mathbb{Q}(0), \mathbb{Q}(1)) \xrightarrow{\text{Tr}} \mathbb{IR}$ , der Scholl's motivische Interpretierung der Höhen-Paarung folgendermaßen reinterpretiert:

$$\begin{array}{ccc} \text{Ext}_{\mathcal{MM}_X}^1(\mathbb{Q}(0), M) \times \text{Ext}_{\mathcal{MM}_X}^1(M, \mathbb{Q}(1)) & \rightarrow & \text{Ext}_{\mathcal{MM}_X}^2(\mathbb{Q}(0), \mathbb{Q}(1)) \xrightarrow{\text{Tr}} \mathbb{IR} \\ \uparrow & & \parallel \\ \text{CH}^n(Y)^0 \times \text{CH}^m(Y)^0 & \longrightarrow & \mathbb{IR}, \end{array}$$

wobei  $M = h^{2n-1}(Y)(n)$  und  $Y$  eine glatte projektive Varietät über  $K$  mit (gewöhnlichen) guten Eigenschaften. Insbesondere ist  $\text{Ext}_{\mathcal{MM}_X}^2(\mathbb{Q}(0), \mathbb{Q}(1)) \neq 0$ .

## W. BAUER:

### Logarithmische algebraische Geometrie

Logarithmische algebraische Geometrie ist eine Erweiterung der alg. Geometrie, die von K. Kato entwickelt wurde und auf Fontaine und Illusie zurückgeht. Ein logarithmisches Schema ist ein Schema  $X$  zusammen mit einem Monoidhomomorphismus  $\alpha : M \rightarrow \mathcal{O}_X^\times$  (auf  $X_{et}$  oder  $X_{zar}$ ), so daß  $\alpha$  einen Isomorphismus  $\alpha^{-1}(\mathcal{O}_X^\times) \rightarrow \mathcal{O}_X^\times$  induziert. Wesentliche Begriffe der alg. Geometrie wie etwa Differentialmodul, glatte oder étale Morphismen etc. lassen sich auf log-Schemata erweitern, und man erhält eine gute Theorie, völlig analog zur klassischen. Ein entscheidender Punkt ist, daß gewisse Klassen singulärer Schemata glatt werden, wenn man sie mit geeigneten log-Strukturen versieht. Ein Standardbeispiel hierfür ist ein Schema mit semistabiler Reduktion über einem diskreten Bewertungsring, wobei die log-Struktur durch die Funktionen gegeben ist, die außerhalb der speziellen Faser invertierbar sind. Anwendungen von log-Strukturen sind Kato's Beweise zu:

- Fontaine-Jannsen-Vermutung über den Zusammenhang zwischen  $p$ -adischer Etale-Kohomologie und De-Rham-Kohomologie in der semi-stabilen Situation (für  $\dim X < (p-1)/2$ )
- Vermutung von Birch and Swinnerton-Dyer: Sei  $K/\mathbb{F}_p$ , Funktionenkörper,  $A/K$  abelsche Varietät mit semi-stabiler Reduktion und  $\# \text{III}(A/K) < \infty$  und  $\# A(K) < \infty$ . Dann gilt:  $L^*(A, 1) = \frac{\# \text{III}(A/K)}{\# A(K) \cdot \# A(K)}$ .

## E. KANI:

### Ends of metric spaces and arithmetic intersection theory

Let  $K$  be a field which is complete w. r. t. a real-valued valuation  $v$  and let  $C$  be a projective, smooth curve over  $K$  with function field  $F$ . The aim of this lecture was to explain that the set

$$P(C) = \{V : V \text{ is a val'n of } F, V|_K = v \text{ and } \kappa(V)/\kappa(v) \text{ transc.}\}$$

of  $v$ -prime divisors carries a natural metric  $d$  with the property that each interval  $[U, V] := \{W \in P(C) : d(U, W) + d(W, V) = d(U, V)\}$ ,  $U, V \in P(C)$  is "linear", i.e., via  $d(U, \cdot)$  isometrically isomorphic to a subset of  $\mathbb{R}$ . For such metric spaces one can develop a theory of ends which is analogous to the usual theory of ends for trees. It is then possible to prove that there exists a canonical isomorphism of topological spaces  $e : C(K) \xrightarrow{\sim} E(P(C))$ , where  $C(K)$  is endowed with the  $v$ -topology and the space  $E(\cdot)$  of ends with a certain limit topology. (Assume here that  $K$  is algebraically closed.) Via this identification, Néron's height pairing on  $\text{Div}^0(C)$  can be extracted by taking limits (along ends):

$$(P_1 - P_2, P_3 - P_4)_v = \frac{1}{2} \lim_{V_i \rightarrow P_i, 1 \leq i \leq 4} [d(V_1, V_3) - d(V_2, V_3) - d(V_1, V_4) + d(V_2, V_4)]$$

Finally, it was explained that  $d$  may be viewed as a "universal arithmetic intersection theory" as follows. If  $\mathcal{C}$  is a normal model of  $C$  over  $\mathcal{O}_v$  with special fibre  $\tilde{\mathcal{C}} = \tilde{\mathcal{C}}_1 \cup \dots \cup \tilde{\mathcal{C}}_n$  and associated valuations  $V_1, \dots, V_n \in P(C)$ , then the intersection matrix

$((C_i, C_j))_{i,j}$  may be computed from  $(d(V_i, V_j))_{i,j}$ , and similarly  $(\bar{P} \cdot C_i)$  (resp.  $(\bar{P} \cdot \bar{Q})$ ),  $P, Q \in C(K)$  may be computed from  $\lambda_{V_i}(V_j, P) = \lim_{V \rightarrow P} \lambda_{V_i}(V_j, V)$  (resp. from  $\lambda_{V_i}(P, Q) = \lim_{V \rightarrow P, W \rightarrow Q} \lambda_{V_i}(V, W)$ ), where  $\lambda_V(U, W) = \frac{1}{2}[d(U, V) + d(V, W) - d(U, W)]$ .

### A. SMIRNOV:

#### Fontaine inequality for torseurs

Let  $N$  be a finite group scheme over  $R$  (ring of integers in a local field  $k$ ),  $X$  be a torseur over  $R$  with respect to  $N$ . It is proved that the split field of  $X$  is not very strongly ramified over  $k$ . Namely,

$$u(X) \leq v(N) + e/(p-1),$$

where  $e$  is the absolute ramification index of  $k$  over  $\mathbb{Q}_p$ ,  $v(N) = \min_{x \in I(N)} v(x)$ ,  $I(N) = \{x \in R \mid x\Omega_N^1 = 0\}$ ,  $v$  the standard valuation of  $k$ ,  $u(X) = \inf\{u \in \mathbb{R} \mid (\text{Gal}(k))^u \text{ acts trivially on the images of all the embeddings of } B \text{ in } \bar{k}\}$ ,  $X = \text{Spec } B$ . Then this inequality is applied to estimate ranks and Shafarevich-Tate groups of  $\text{Jac}(x^p + y^p = 1)$  over some cyclotomic extensions.

### J. F. MESTRE

#### Elliptic curves of finite rank

One conjectures that the rank of elliptic curves defined over  $\mathbb{Q}$  is not bounded. One method to attack this problem is to consider an analogue of this conjecture over  $\mathbb{Q}(t)$ . One can prove the following theorem:

**Theorem:** There exists an elliptic curve defined over  $\mathbb{Q}(t)$  with non-constant modular invariant which possesses twelve over  $\mathbb{Q}(t)$  rational independent points.

**Corollary:** There exist infinite elliptic curves defined over  $\mathbb{Q}$  (pairwise not isomorphic over  $\bar{\mathbb{Q}}$ ) such that the rank of the Mordell-Weil-group is  $\geq 12$ .

By specialization of  $t$ , Stephane Famigia was able to find two elliptic curves defined over  $\mathbb{Q}$  with rank  $\geq 19$ .

### J. A. ANTONIADIS:

#### Artinsche $L$ -Funktionen zu tetraedrischen Darstellungen

Es wurde eine Methode vorgestellt, wie man zweidimensionale irreduzible ungerade  $A_4$ -Darstellungen konstruiert und wie man die Koeffizienten der entsprechenden Artinschen  $L$ -Reihe  $L(s, \rho)$  berechnen kann.

### S. BÖGE:

#### Das Einbettungsproblem $SL(2, l) \rightarrow PSL(2, l)$

$L/K$  sei eine endliche algebraische Erweiterung von Zahlkörpern, und  $K$  habe nur eine dyadische Stelle. Die 2-Sylowgruppen von  $G \cong \text{Gal}(L/K)$  seien Diedergruppen.  $G$  werde zweiblättrig überlagert von  $\tilde{G}$ , und die 2-Sylowgruppen von  $\tilde{G}$  seien verallge-

meinte Quaternionengruppen. Das Einbettungsproblem

$$\begin{array}{ccc} G(\tilde{L}/K) & \xrightarrow{\text{res}_L} & G(L/K) \\ \downarrow & & \downarrow \cong \\ \tilde{G} & \longrightarrow & G \end{array}$$

ist genau dann lösbar, wenn I und II beide erfüllt sind:

- I. Die reellen Stellen von  $K$  besitzen nur reelle Fortsetzungen auf  $L$ .
- II. Für jede nicht dyadische Stelle  $\varphi$  von  $K$  gilt: Wenn die 2-Sylowgruppen der Zerlegungsgruppen  $G_{\mathbb{R}}(\mathbb{R}/\varphi)$  zyklisch sind, dann muß die höchste in der Verzweigungsordnung  $e$  (von  $\varphi$  in  $L/K$ ) aufgehende Potenz von 2 auch in  $(q-1)/2$  auftreten ( $q = N\varphi$ ); sind sie nicht zyklisch, dann muß diese Potenz in  $(q+1)/2$  auftreten.

### J. NEUKIRCH:

#### Mikroprimstellen

Die Mikroprimstellen entstehen in kanonischer Weise bei der Betrachtung der abstrakten Klassenkörpertheorie und dienen der Erklärung des Reziprozitätsgesetzes der lokalen, globalen, aber auch vielleicht der höherdimensionalen Klassenkörper.

### M. JARDEN:

#### Effective counting of points on definable sets over finite fields

(Report on a joint work with M. Fried and D. Haran which is due to appear in a special volume of the Israel Journal of Mathematics dedicated to Field Arithmetic)

The goal of the lecture was to present the following theorem and to indicate the three steps of its proof.

**Theorem.** Let  $\phi(X, Y) = \phi(X_1, \dots, X_m, Y_1, \dots, Y_n)$  be a formula in the language of rings. For each prime power  $q$  and each  $\underline{b} \in \mathbb{F}_q^m$  let  $N_q(\underline{b}) = \#\{\underline{a} \in \mathbb{F}_q^n \mid \mathbb{F}_q \models \phi(\underline{a}, \underline{b})\}$ . Then we can effectively find a positive constant  $c$ , formulas  $\theta_1(Y), \dots, \theta_k(Y)$  in the language of rings, positive rational numbers  $\mu_1, \dots, \mu_k$ , and integers  $r_1, \dots, r_k \in \{0, 1, \dots, m\}$  with the following property: For every  $q$  and each  $\underline{b} \in \mathbb{F}_q^n$  there exists a unique  $1 \leq i \leq k$  such that  $\mathbb{F}_q \models \theta_i(\underline{b})$  and  $N_q(\underline{b})$  is either 0 or satisfies:  $|N_q(\underline{b}) - \mu_i q^{r_i}| \leq c^{r_i - \frac{1}{2}}$ .

The existence of  $c, \theta_i(Y), \mu_i$  and  $r_i$  was first proved by Z. Chatzidakis, L. v. d. Dries and A. Macintyre by model theoretic methods.

### R. SCHOOF:

#### Counting points on elliptic curves over finite fields

One can efficiently calculate the number of points on an elliptic curve over  $\mathbb{Z}/p\mathbb{Z}$  by considering the action of the Frobenius endomorphism on  $l$ -torsion points for several small primes  $l$ . The calculation boils down to computing certain powers modulo the divisor polynomial which has degree  $(l^2 - 1)/2$ .

Recently, N. Elkies came up with a practical improvement of this algorithm. He ex-

ploits certain modular functions. A. O. L. Atkin implemented these improvements on a computer and is able to compute the number of points on an elliptic curve over  $\mathbb{Z}/p\mathbb{Z}$  where  $p$  is a 200 decimal digit prime.

## I. KIMING:

### Congruences of Ramanujan type

For the numbers  $p_r(n)$ ,  $r \in \mathbb{N}$ ,  $n \in \mathbb{N}_0$  defined by  $\prod_{n=1}^{\infty} (1 - q^n)^{-r} = \sum_{n=0}^{\infty} p_r(n)q^n$  (formal power series), we study congruences of the type:  $p_r(ln + a) \equiv 0 \pmod{l}$  for all  $n \in \mathbb{N}_0$ , where  $a \in \mathbb{N}$  and  $l \geq 5$  is a prime number. The motivation is that these numbers occur in the modular representation theory of symmetric groups and that congruences of the above type have certain consequences in that theory. Three cases, for  $r = 1$ , are classical and were obtained by Ramanujan:  $p(5n+4) \equiv 0 \pmod{5}$ ,  $p(7n+5) \equiv 0 \pmod{7}$ ,  $p(11n+6) \equiv 0 \pmod{21}$  for all  $n \in \mathbb{N}_0$ . Here  $p = p_1$  is the partition function. There are examples for  $r > 1$ :  $p_3(11n+7) \equiv 0 \pmod{11}$ ,  $p_{13}(17n+14) \equiv 0 \pmod{17}$ ,  $p_7(19n+9) \equiv 0 \pmod{19}$ ; ... for all  $n \in \mathbb{N}_0$ . Using classical identities of Euler and Jacobi, we show that the situation is trivial to analyze for  $r = l-1$  or  $r = l-3$ . For the other "exceptional" cases we give a necessary condition for the occurrence of congruences of the above type:

**Theorem:** Suppose that  $l \geq 5$  is a prime number,  $a, r \in \{1, \dots, l-1\}$ ,  $v \notin \{l-1, l-3\}$  and that  $p_r(ln + a) \equiv 0 \pmod{l}$  for all  $n \in \mathbb{N}_0$ . Then:  $r$  is odd and  $24a \equiv r \pmod{l}$ .

## A. LEUTBECHER:

### Über die Lenstra-Konstanten von Zahlringen

Diese Invarianten  $M_k(\Gamma)$  ( $k \in \mathbb{N}$ ) verallgemeinern die Cliquenzahl  $M_1(\Gamma)$  einfacher Graphen. Sie erfüllen die folgenden Abschätzungen und Gleichungen

$$M_1(\Gamma) \leq \frac{M_k(\Gamma)}{k} \leq \sup_k \frac{M_k(\Gamma)}{k} = \lim_{k \rightarrow \infty} \frac{M_k(\Gamma)}{k} =: M_*(\Gamma)$$

Für Paare  $(R, U)$ , bestehend aus einem kommutativen Ring  $R$  und einer Untergruppe  $U \ni -1$  von  $R^\times$  werden sie bezogen auf die Györy-Graphen  $\Gamma(R, U)$  mit der Eckenmenge  $R$  und der Adjazenz  $a \sim b \Leftrightarrow a - b \in U$ . Unter Verwendung der Funktoreigenschaften von  $\Gamma(R, U)$  wird bewiesen der

**Satz:** Für die Ganzheitsringe reellquadratischer Zahlkörper und kubischer Zahlkörper vom Einheitenrang 1 gilt

$$M_*(\mathbb{Z}_K, \mathbb{Z}_K^\times) = M_*(\mathcal{O}, \mathcal{O}^\times) = \inf_{I \subset \mathcal{O}} M_*(\mathcal{O}/I, (\mathcal{O}^\times + I)/I)$$

Darin bezeichnet  $\mathcal{O}$  die von  $\mathbb{Z}_K^\times$  erzeugte Ordnung des betreffenden Zahlkörpers.

## F. POP:

### Ein Riemannscher Satz für Divisoren mit rationalen Komponenten

Sei  $K$  ein beliebiger Körper und  $X/K$  eine glatte projektive irreduzible Kurve mit  $X(K) \neq \emptyset$ . Ein r. c. Riemannscher Satz besteht darin, zu beschreiben den Teilraum  $|nD|^{r.c.} \subseteq |nD|$ , der aus allen zu  $nD$  linear äquivalenten Divisoren  $\sum_i P_i \sim nD$  ( $P_i \in X(K)$ ) besteht. Hierzu kann man folgendes beweisen:

Satz: Zu beliebigen Schranken  $g, N$  existiert eine natürliche Zahl  $g$  mit der Eigenschaft: Sei  $K$  ein endlicher (lokaler) Körper und sei das Geschlecht von  $X$  kleiner oder gleich  $g$  (und zusätzlich habe die Gruppe der Zusammenhangskomponenten des Neronschen Modells von  $X$  Ordnung  $\leq N$ ). Ferner sei  $\langle X(K) \rangle \subseteq J(K)$  die Gruppe aller Divisorenklassen der Form  $\sum_i (P_i - P_0)$  mit  $P_0 \in X(K)$  fest. Dann gilt:

$$(1) \langle X(K) \rangle = \sum_{i \leq g} \text{class}(P_i - P_0)$$

$$(2) \#(J(K)/\langle X(K) \rangle) < g$$

Insbesondere ist  $|nD|^{r.c.} \neq \emptyset$  für  $n$  Vielfaches von  $g$ !

Berichterstatter: B. Köck (Karlsruhe)

Tagungsteilnehmer

Prof.Dr. Jannis A. Antoniadis  
Dept. of Mathematics  
University of Crete  
P. O. Box 1470  
  
Iraklion Crete  
GREECE

Prof.Dr. Salvador Comalada  
Institut für Experimentelle  
Mathematik  
Universität-Gesamthochschule Essen  
Ellernstr. 29  
  
W-4300 Essen 12  
GERMANY

Dr. Werner Bauer  
Fachbereich 7: Mathematik  
U-GHS Wuppertal  
Gaußstr. 20  
Postfach 10 01 27  
  
W-5600 Wuppertal 1  
GERMANY

Prof.Dr. Christopher Deninger  
Mathematisches Institut  
Universität Münster  
Einsteinstr. 62  
  
W-4400 Münster  
GERMANY

Prof.Dr. Eva Bayer-Fluckiger  
Laboratoire de Mathématiques  
Université de Franche-Comté  
16, Route de Gray  
  
F-25030 Besançon Cedex

Prof.Dr. Graham R. Everest  
School of Mathematics & Physics  
University of East Anglia  
University Plain

Prof.Dr. Sigrid Böge  
Mathematisches Institut  
Universität Heidelberg  
Im Neuenheimer Feld 288/294  
  
W-6900 Heidelberg 1  
GERMANY

Dr. Matthias Flach  
Mathematisches Institut  
Universität Heidelberg  
Im Neuenheimer Feld 288  
  
W-6900 Heidelberg 1  
GERMANY

Prof.Dr. Harvey Cohn  
Department of Mathematics  
The City College of New York  
Convent Avenue at 138th Street  
  
New York , NY 10031  
USA

Prof.Dr. Gerhard Frey  
Institut für Experimentelle  
Mathematik  
Universität-Gesamthochschule Essen  
Ellernstr. 29  
  
W-4300 Essen 12  
GERMANY

Prof.Dr. Albrecht Fröhlich  
63, Drax Avenue  
Wimbledon  
GB- London SW 20 0EZ

Prof.Dr. Wolfram Jehne  
Mathematisches Institut  
Universität zu Köln  
Weyertal 86-90

W-5000 Köln 41  
GERMANY

Prof.Dr. Wulf-Dieter Geyer  
Mathematisches Institut  
Universität Erlangen  
Bismarckstr. 1 1/2  
  
W-8520 Erlangen  
GERMANY

Prof.Dr. Ernst Kani  
Department of Mathematics and  
Statistics  
Queen's University

Kingston, Ontario K7L 3N6  
CANADA

Prof.Dr. Barry W. Green  
Mathematisches Institut der  
Universität Heidelberg  
Im Neuenheimer Feld 288  
  
W-6900 Heidelberg 1  
GERMANY

Prof.Dr. Ian Kiming  
Institut für Experimentelle  
Mathematik  
Universität-Gesamthochschule Essen  
Ellernstr. 29

W-4300 Essen 12  
GERMANY

Prof.Dr. Franz Halter-Koch  
Institut für Mathematik  
Karl-Franzens-Universität  
Heinrichstr. 36  
  
A-8010 Graz

Guido Kings  
Mathematisches Institut  
Universität Münster  
Einsteinstr. 62

W-4400 Münster  
GERMANY

Prof.Dr. Moshe Jarden  
Institute for Advanced Studies  
Hebrew University of Jerusalem  
Givat Ram  
  
91904 Jerusalem  
ISRAEL

Dr. Ernst Kleinert  
Mathematisches Seminar  
Universität Hamburg  
Bundesstr. 55

W-2000 Hamburg 13  
GERMANY

Prof.Dr. Norbert Klingen  
Mathematisches Institut  
Universität zu Köln  
Weyertal 86-90

W-5000 Köln 41  
GERMANY

Prof.Dr. Heinrich-Wolfg. Leopoldt  
Mathematisches Institut II  
Universität Karlsruhe  
Kaiserstr. 12

W-7500 Karlsruhe 1  
GERMANY

Prof.Dr. Helmut Koch  
Arbeitsgruppe Geometrie und  
Zahlentheorie  
Humboldt-Universität Berlin  
Mohrenstr. 39  
  
0-1086 Berlin  
GERMANY

Prof.Dr. Armin Léutbecher  
Mathematisches Institut  
TU München  
PF 20 24 20, Arcisstr. 21

W-8000 München 2  
GERMANY

Bernhard Köck  
Mathematisches Institut II  
Universität Karlsruhe  
Englerstr. 2  
  
W-7500 Karlsruhe 1  
GERMANY

Prof.Dr. Falko Lorenz  
Mathematisches Institut  
Universität Münster  
Einsteinstr. 62

W-4400 Münster  
GERMANY

Prof.Dr. Erich Lamprecht  
Fachbereich 9 - Mathematik  
Universität des Saarlandes  
Bau 27

W-6600 Saarbrücken  
GERMANY

Prof.Dr. Manohar L. Madan  
Department of Mathematics  
Ohio State University  
231 West 18th Avenue

Columbus , OH 43210-1174  
USA

Prof.Dr. Johann B. Leicht  
Mathematisches Institut  
Universität Heidelberg  
Im Neuenheimer Feld 288/294

W-6900 Heidelberg 1  
GERMANY

Dr. Gunter Martin Malle  
Interdisziplinäres Zentrum  
für Wissenschaftliches Rechnen  
Universität Heidelberg  
Im Neuenheimer Feld 368

W-6900 Heidelberg 1  
GERMANY

**Prof.Dr. B.Heinrich Matzat**  
Interdisziplinäres Zentrum  
für Wissenschaftliches Rechnen  
Universität Heidelberg  
Im Neuenheimer Feld 368

W-6900 Heidelberg 1  
GERMANY

**Prof.Dr. Jean-François Mestre**  
UFR de Mathématiques  
Université de Paris VII  
2, place Jussieu

F-75251 Paris Cedex 05

**Prof.Dr. Tauno Metsaenkylae**  
Institute of Mathematical Sciences  
University of Turku

SF-20500 Turku

**Prof.Dr. Katsuya Miyake**  
Dept. of Mathematics  
College of General Education  
Nagoya University  
Chikusa-Ku

Nagoya 464-01  
JAPAN

**Prof.Dr. Enric Nart**  
Dept. de Matemáticas  
Universidad Autonoma de Barcelona

E-08193 Bellaterra, Barcelona Catalunya

**Prof.Dr. Jürgen Neukirch**  
Fakultät für Mathematik  
Universität Regensburg  
Postfach 397  
Universitätsstr. 31

W-8400 Regensburg  
GERMANY

**Prof.Dr. Robert W. K. Odoni**  
Dept. of Mathematics  
University of Glasgow  
University Gardens

GB- Glasgow G12 8QW

**Prof.Dr. Hans Opolka**  
Institut für Algebra und  
Zahlentheorie  
TU Braunschweig  
Pockelsstr. 14

W-3300 Braunschweig  
GERMANY

**Dr. Florian Pop**  
Mathematisches Institut  
Universität Heidelberg  
Im Neuenheimer Feld 288/294

W-6900 Heidelberg 1  
GERMANY

**Dr. Hans-Peter Rehm**  
Mathematisches Institut II  
Universität Karlsruhe  
Englerstr. 2

W-7500 Karlsruhe 1  
GERMANY

Prof.Dr. Jürgen Ritter  
Institut für Mathematik  
Universität Augsburg  
Universitätsstr. 8

W-8900 Augsburg  
GERMANY

Prof.Dr. Claus-Günther Schmidt  
Mathematisches Institut II  
Universität Karlsruhe  
Kaiserstr. 12

W-7500 Karlsruhe 1  
GERMANY

Prof.Dr. Peter Roquette  
Mathematisches Institut  
Universität Heidelberg  
Im Neuenheimer Feld 288/294

W-6900 Heidelberg i  
GERMANY

Prof.Dr. René Schoof  
Dipartimento di Matematica  
Univers. degli Studi di Trento  
I-38050 Povo (Trento)

Dr. Hans-Georg Rück  
Institut für Experimentelle  
Mathematik  
Universität-Gesamthochschule Essen  
Ellernstr. 29

W-4300 Essen 12  
GERMANY

Dr. Vladimir A. Smirnov  
St. Petersburg Branch of Steklov  
Mathematical Institute - LOMI  
Russian Academy of Science  
Fontanka 27

191011 St. Petersburg  
RUSSIA

Prof.Dr. Reinhard Schertz  
Institut für Mathematik  
Universität Augsburg  
Universitätsstr. 8

W-8900 Augsburg  
GERMANY

Michael Spieß  
Fakultät für Mathematik  
Universität Regensburg  
Postfach 397  
Universitätsstr. 31

W-8400 Regensburg  
GERMANY

Dr. Alexander Schmidt  
Mathematisches Institut  
Universität Heidelberg  
Im Neuenheimer Feld 288/294

W-6900 Heidelberg 1  
GERMANY

Prof.Dr. Michael J. Taylor  
Dept. of Mathematics  
UMIST (University of Manchester  
Institute of Science a. Technology)  
P. O. Box 88

GB- Manchester , M60 1QD

Annette Werner  
Mathematisches Institut  
Universität Münster  
Einsteinstr. 62  
  
W-4400 Münster  
GERMANY

Prof.Dr. Kay Wingberg  
Mathematisches Institut  
Universität Heidelberg  
Im Neuenheimer Feld 288/294  
  
W-6900 Heidelberg 1  
GERMANY

Prof. Dr. Ernst-Wilhelm Zink  
Arbeitsgruppe Geometrie und  
Zahlentheorie  
Humboldt-Universität Berlin  
Mohrenstr. 39  
  
D-1086 Berlin  
GERMANY