MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 16/1983

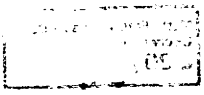
Arithmetik elliptischer Kurven

10.4. bis 16.4.1983

Die Tagung über die Arithmetik elliptischer Kurven fand unter der Leitung von Herrn J. Coates (Paris), Herrn A. Fröhlich (London) und Herrn P. Roquette (Heidelberg) statt. Das Ziel der Tagung war, einem großen Kreis interessierter Mathematiker einen Überblick über den derzeitigen Kenntnisstand in diesem Bereich der Mathematik zu geben.

Zu der Tagung erschienen 56 Mathematiker, darunter 32 Gäste aus dem Ausland. Durch die Anwesenheit führender Fachleute konnten allerneuerste Forschungsergebnisse vorgestellt und ausgetauscht werden.

Das Programm der ersten Tage sah je zwei Vorträge der Herren Kneser (Einführung), Tate (kanonische Höhenpaarungen), Lichtenbaum (Iwasawatheorie abelscher Varietäten), Schneider (p-adische Höhenpaarungen), Harder (spezielle Werte von L-Reihen), Schappacher (Konstruktion p-adischer L-Reihen) und Coates (Hauptvermutung) vor. Der Themenkreis der letzten beiden Tage umfaßte verschiedene Aspekte mit Vorträgen von Mestre, Bernadi, Zagier, Cassels, Birch und Stephens. Zusätzlich wurden an zwei Abenden Vorträge von Herrn Zagier und Herrn Husemöller gehalten.



Vortragsauzüge

M. KNESER:

Two introductory lectures, or: "What everybody should know before going to a conference on elliptic curves".

Review of fundamental notions, facts and conjectures. Basic reference: [T], J. Tate, Inventions 23 (1974).

1. Weierstrass models ([T], §2)

2. Elliptic curves over local fields ([T], §6)

Minimal Weierstrass model for an elliptic curve E over a local field k_v with residue class field $\bar{k}_v$. Reduced curve $\bar{E}/\bar{k}_v$. Good reduction, split and non-split multiplicative reduction, additive reduction. Subgroups $E_1(k_v) \subset E_0(k_v) \subset E(k_v)$.

3. Heights ([T], §7)

Naive height and canonical (Néron-Tate) height on an elliptic curve E over a number field k. Deduction of the Mordell-Weil theorem from the finiteness of $E(k)/mE(k)$.

4. The Selmergroups $S^{(m)}(E)$ and the Tate-Šafarevič-groups $Ш(E)$ ([T], §7)

Definitions. The exact sequence

$$0 \to E(k)/mE(k) \to S^{(m)}(E) \to Ш(E)_m \to 0 .$$

Problems of computation.

5. The conjectures of Birch and Swinnerton - Dyer ([T], §8)

Definition of the Hasse-Weil L-function $L(E,s)$ for $\operatorname{Re} s > \frac{3}{2}$.

Statement of the Birch and Swinnerton-Dyer conjectures:

(A) $L(E,s)$ has an analytic continuation beyond $s = 1$ and satisfies a functional equation for $s \leftrightarrow 2 - s$.

- This is known to hold for curves with complex multiplication.

(B) $L(E,s)$ has a zero at $s = 1$ of order equal to the rank r of $E(k)$.

- This has been confirmed in many cases.

(C) $Ш(E)$ is finite.

- This has not been proved for any single elliptic curve. Only certain p-primary parts have been computed.

(D) $$\lim_{s \to 1} (s-1)^{-r} L(E,s) = |E(k)_{tor}|^{-2} |Ш(E)| \det < P_i, P_j > 2^{r_2} |d_k|^{-\frac{1}{2}} \prod_v m_v ,$$

where $P_1,\dots,P_r$ are generators of $E(k)$ modulo the torsion subgroup $E(k)_{tor}$, $<\ ,\ >$ is the canonical height pairing, r_2 the number of complex places of k, d_k its absolute discriminant, and the finitely many factors m_v depend on an invariant differential ω on E and the index $[E(k_v) : E_0(k_v)]$.

6. Tamagawa numbers

Interpretation of (D) as a formula for the Tamagawa numbers $\tau(X)$ of a certain extension X of E by a torus $\mathbb{G}_m^r$.

$$\tau(X) = |\,Pic(X)_{tor}\,| \cdot |Ш(X)|^{-1}$$

Basic reference: [T], J. Tate, Inventions 23 (1974),
B. Birch, N. Stephens, Topology 5 (1966),
S. Bloch, Inventions 58 (1980),
P. Roquette, Analytic theory of elliptic functions over local fields, Hamburger Math. Einzelschr. (1970),
J. Tate in "Modular Functions of One Variable IV" (Antwerpen 1972), LN 476.

J. TATE:

Canonical Height Pairings

A an elliptic curve over a number field k. A place v of k is ordinary for A if A has either good ordinary reduction or has (possibly twisted) multiplicative reduction at v. Let S be a finite set of ordinary places for A. Let $A_S = \{P \in A(k) \mid$ the reduction $\bar{P}_v$ of P at v is 0 for all $v \in S.\}$. Let $A_S^0 = \{P \in A_S \mid \bar{P}_v$ is in the connected component of the special fiber of Néron's model for A at all finite $v\}$. Let $C^S = J/k^*J^S$, where J is the idèle group of k and where $J^S = \{(a_v) \in J/|a_v|_v = 1$ for $v \notin S$ and $a_v = 1$ for $v \in S\}$

Both the classical real height and the recent p-adic-height came from a canonical pairing

$$<\ ,\ >_S : A_S^0 \times A_S \to C^S$$

which is constructed by using, for $v \notin S$, the local symbols of Néron (Annals of Math (1965), 244-331) and for $v \in S$ those

of Mazur-Tate (Canonical Height Pairings via Biextensions, to appear this June in Arithmetic and Geometry; papers dedicated to I.R. Shafarevitch on the occasion of his 60th birthday. (two Vols.) in the Birkhäuser "Progress in Math." (green) series.

Functional properties of $\langle , \rangle_S$: 1) compatible with increasing S 2) symmetric 3) If $f : A \to B$ has $f' : B \to A$ as dual, then $\langle fP, Q \rangle_S = \langle P, f'Q \rangle_S$. 4) If $i : K \subset K'$, then $i\langle P, Q \rangle_S = \langle iP, iQ \rangle_{S'}$, if S' = places above S, and also $\langle Tr_{K'/K} P', Q \rangle_S = N_{K'/K} \langle P', iQ \rangle_{S'}$.

Suppose $\lambda : C \to \mathbb{R}$ or $\mathbb{Q}_p$ is a continous homomorphism such that, in case of $\mathbb{Q}_p$, λ is ramified only at ordinary places. Then there is an S such that λ factors through C^S, and hence there is a unique pairing $\langle , \rangle_\lambda : A(k) \times A(k) \to \mathbb{R}$ or $\mathbb{Q}_p$ coinceding with $\lambda \circ \langle , \rangle$ on $A_S^0 \times A_S$ for any such S. In case of $\mathbb{R}$ with $\lambda(x) = \Sigma_v \log \|x_v\|_v$ this is the classical real-valued height pairing discussed by Kneser above. In case of $\mathbb{Q}_p$ we have the λ-p-adic height; it coincides with that defined by Schneider in case of ordinary good reduction, and earlier by Bernardi in some CM cases. Choosing a basis $\{P_i\}_{1 \le i \le r}$ for $A(k)$ mod torsion we get an interesting function $\delta(\lambda) = \det_{1 \le i \le r} \langle P_i, P_j \rangle_\lambda$; It is a form of degree r on our space of λ's. What are its zeros? The corresponding $\mathbb{Z}_p$-extensions should behave very specially for A. Is the homogeneous form $S(\lambda)$, up to a constant, the leading form of the p-adic $L(A, \chi_0 e^\lambda)$, viewed as function of λ?

Theorem (Mazur-Tate, Cristante, Norman,...) Let k be a local field of res. char. $p \neq 0$ with ring of integers $\mathcal{O}$. Suppose A is an ell. curve defined over k and ordinary. Let A^f be the formal group of A over $\mathcal{O}$ and t a good local parameter at 0 so that $A^f = \mathrm{Spf}\, R$, when $R = \mathcal{O}[[t]]$. If $p \neq 2$, there exists a unique $\sigma \in R$ such that $\sigma \equiv t \pmod{t^2}$ and such that given a division $\mathcal{M} = \Sigma m_i (P_i)$ with $P_i \in A_f(\mathcal{O}) \subset A(k)\ \forall i$ and with $\Sigma m_i = 0$ and $\Sigma m_i P_i = 0$, the function $P \mapsto \pi_i \sigma(P - P_i)^{m_i}$ is the restriction to $A^f(\mathcal{O})$ of a rational function on A defined over k with division $\mathcal{M}$.

This canonical p-adic σ-function can be used to compute local p-adic heights at places above p just as the Weierstraß σ-function is used to compute the archmedean height at archmedean places.

S. LICHTENBAUM:

Flat Cohomology and Iwasawa theory of abelian varieties (an introduction to the work of Peter Schneider)

I. Basic facts about étale and flat cohomology groups.

These groups are cohomological functors, a long exact sequence of relative cohomology exists, they satisfy an excision property, a Hochschild-Serre spectral sequence exists for Galois (étale) coverings, étale cohomology and Galois cohomology coincide for fields, flat and étale cohomology coincide for smooth group schemes.

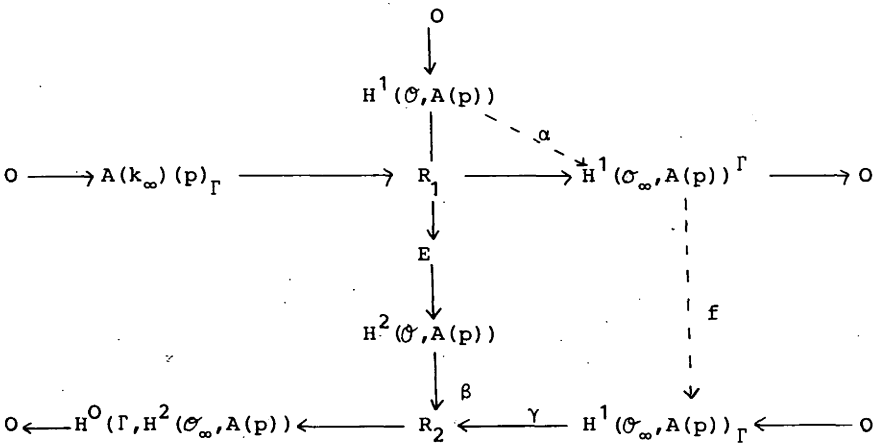
II. The dual of the (cohomological) Selmer group.

Let k be a number field, k_∞ a $\mathbb{Z}_p$ $(=\Gamma)$-extension of k. Let A_k be an abelian variety over k with good reduction at all primes over p and ordinary reduction at those primes which ramify in k_∞. Let $\mathcal{O}$ (resp. $\mathcal{O}_\infty$) be the ring of integers in k (resp. k_∞). Let A be the Néron model of A_k over $\mathcal{O}$ and let $A(p)$ be the p-torsion subsheaf of A. The cohomological Selmer group over $\mathcal{O}$ (resp. $\mathcal{O}_\infty$) is defined to be $H^1(\mathcal{O},A(p))$, (resp. $H^1(\mathcal{O}_\infty,A(p))$), where H^1 denotes flat cohomology. Letting $\Lambda = \mathbb{Z}_p[[\Gamma]]$, the dual, H, of the Selmer group over $\mathcal{O}_\infty$ is conjectured to be Λ-torsion if k_∞ is the cyclotomic Γ-extension. Its characteristic power series should be equal up to a unit to the p-adic L-function of the Abelian variety. Since we have the exact sequence

$$0 \to A(k) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(\mathcal{O},A(p)) \to H^1(\mathcal{O},A)(p) \to 0$$

the Selmer group is closely related to the Mordell-Weil group $A(k)$ and the Tate-Šafarevič group $Ш_k(A)$.

III. By using the cohomological facts from (I), together with computations of Galois cohomology over local fields, we obtain the basic "descent diagram":



where R_1 and R_2 are equivariant cohomology groups, and α and β are quasi-isomorphisms.

IV. The algebraic height pairing.

Let $\tilde{A}$ be the dual abelian variety of A. Then the sequence of maps:

$$H^1(\mathcal{O},T_p(\tilde{A})) \simeq \text{(flat duality)}\ H^2(\mathcal{O},A(p))^* \xrightarrow{(\beta^*)^{-1}} R_2^* \xrightarrow{\gamma^*} (H^1(\mathcal{O}_\infty,A(p))_\Gamma)^*$$

$$\downarrow f^*$$

$$\text{Hom}\,(H^1(\mathcal{O},T_p(A)),\mathbb{Z}_p) \longleftarrow H^1(\mathcal{O}_\infty,A(p))^* \longleftarrow (H^1(\mathcal{O}_\infty,A(p))^\Gamma)^*$$

induces the algebraic height pairing:

$$H^1(\mathcal{O},T_p(\tilde{A})) \times H^1(\mathcal{O},T_p(A)) \to \mathbb{Q}_p\ .$$

References: Mazur, Inventions 18 (1972)
Schneider, Inventions 71 (1983)
Schneider, p-adic Height Pairings II (handwritten manuscript).

P. SCHNEIDER:

Iwasawa theory of abelian varieties

Let A/k be an abelian variety over the number field k which has

ordinary good reduction at all primes above a given odd prime number p. Let k_∞/k be the cyclotomic $\mathbb{Z}_p$-extension, $\mathcal{O}_\infty$ its ring of integers, $\Gamma := \mathrm{Gal}(k_\infty/k)$ the Galois group, $\gamma \in \Gamma$ a topological generator, and $K : \Gamma \to \mathbb{Z}_p^\times$ the cyclotomic character. As shown in Lichtenbaum's lecture the Pontrjagin dual

$$H := H^1(\mathcal{O}_\infty, A(p))^*$$

of the first flat cohomology group over $\mathcal{O}_\infty$ of the p-primary part of the Néron model of A is our basic Γ-module. If H is $\mathbb{Z}_p[[\Gamma]]$-torsion we define the Iwasawa L-function of A at p by

$$L_p(A,s) := p^{\mu(H)} \cdot \det(K(\gamma)^{1-s} - \gamma;\ H \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \qquad (s \in \mathbb{Z}_p)\ .$$

Furthermore let $\langle , \rangle_p : \tilde{A}(k) \times A(k) \to \mathbb{Q}_p$ denote the canonical p-adic height pairing as defined in Tate's lecture ($\tilde{A}/k$ the dual abelian variety). Then the following theorem (which can be viewed as an analogue of the Birch/Swinnerton-Dyer conjecture) was proved.

Theorem: Assume that $\langle , \rangle_p$ is nondegenerate and that $Ш_k(A)(p)$ is finite. We then have:

i. H is $\mathbb{Z}_p[[\Gamma]]$-torsion;

ii. $L_p(A,s)$ has a zero of exact multiplicity $\rho := \mathrm{rank}\ A(k)$ at $s = 1$;

iii. $$\left| [L_p(A,s)\cdot(s-1)^{-\rho}]_{s=1} \right|_p^{-1} = \frac{\#Ш_k(A)(p) \cdot |\det \langle , \rangle_p|_p^{-1}}{\#A(k)(p)\ \ \#\tilde{A}(k)(p)} \cdot \prod_{\mathfrak{p}\mid\infty} \#\pi_{\mathfrak{p}}(A)(p)$$

$$\cdot \Big(\prod_{\mathfrak{p}\mid p} \#A(K_{\mathfrak{p}})(p) \Big)^2$$

($K_{\mathfrak{p}}$ residue class field at $\mathfrak{p}$, $\pi_{\mathfrak{p}}(A)$ group of rational connected components of the reduction of A at $\mathfrak{p}$).

Remark: The theorem easily generalizes to any other $\mathbb{Z}_p$-extension. The proof is naturally divided into two steps. In the first step one proves the theorem replacing the canonical by the algebraic p-adic height pairing. This is done by a careful analysis of the descent diagram established in Lichtenbaum's lecture. In the second step one shows that the algebraic height is equal to the canonical one. This requires the development of a new cohomology theory which somewhat lies between etale and flat cohomology. In any case, it allows to modify sheaves "at the primes above p". Such a modification of the multiplicative group sheaf using the notion of local universal

norms leads to the definition of a degree map on a certain modified Picard group to $\mathbb{Z}_p$ and to an expression of the canonical height as a certain Yoneda pairing followed by that degree map. The rest is a subtle cohomological procedure to compare that Yoneda pairing with the algebraic height.

References: see Lichtenbaum's lecture
B. Mazur/J. Tate "Canonical Height Pairings via Biextensions", preprint B. Perrin-Riou, Inv. math. (1982)
P. Schneider, Inv. math. 69 (1982).

G. HARDER:

L-functions of elliptic curves and special values of L-functions

The conjecture of Birch and Swinnerton-Dyer predicts that the arithmetic of an elliptic curve E/k over a number field k is strongly influenced by the behaviour of the Hasse-Weil L-function $L(E/k,s)$ at the special point $s = 1$. If for instance $L(E/k,s) \neq 0$ then it says $L(E/k,1) = \Omega_\infty \times$ rational number.

There is only one method known to establish the analytic continuation of an "arithmetic" L-function namely to relate it to an automorphic L-function. In this case there are two methods to do this which also provides the information about the special values.
1. Method: Our curve E is called a Weil curve if it is defined over $\mathbb{Q}$ and if we have a projection of the modular curve $X_0(N)$:

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

Then the pull back of the differential ω_E on E over $\mathbb{Q}$ is a modular form $2\pi i\, f(z)dz$ of weight two on $\Gamma_0(N)$. The Eichler-Shimura congruence relations tell us that in this case

$$\frac{\Gamma(s)}{(2\pi)^s} L(E/\mathbb{Q},s) = L(f,s) = \int_0^\infty f(iy) y^s \frac{dy}{y}$$

$$= \frac{1}{(2\pi)^s} \sum_{n=1}^{\infty} \frac{a_n}{n^s} \int_{\pi An}^{\infty} e^{-y} y^s \frac{dy}{y} \pm \frac{N^{1-s}}{(2\pi)^{1-s}} \sum_{n=1}^{\infty} \frac{a_n}{n^{2-s}} \int_{\frac{\pi n}{AN}}^{\infty} e^{-y} y^s \frac{dy}{y}$$

for $A > 0$.

The formula for the special value at $s = 1$ can be interpreted as period integral

$$L(E/\mathbb{Q},1) = -2\pi \int_0^{\infty} f(y)\,dy = \int_0^{i\infty} \omega$$

where ω is the algebraic differential on $X_0(N)$. This proves $L(E/\mathbb{Q},1) \cdot \Omega_{\infty}^{-1} \in \mathbb{Q}$.

2. Method: If our curve E/k has complex multiplication by a field k_1, then the Hasse-Weil L-function is a L-function or a product of two L-functions attached to Grössencharacters of type A_0, hence related to automorphic forms on the group $GL(1)$ or $GL(2)$.

Now we assume that $k = k_1$ and that $\mathcal{O}_k \xrightarrow{\sim} \mathrm{End}_k(E)$. One has $L(E/\mathbb{Q},s) = L_k(\psi,s)\, L_k(\bar{\psi},s)$ where ψ is a Grössencharacter:

$$\psi : J_k/k^* \to \mathbb{C}$$
$$\psi : (z,1,\ldots) \mapsto z^{-1}$$
$$\psi : I_k^f \text{ (group of finite idèles)} \to k^* \to \mathbb{C}\ .$$

Then we are interested in the special values $L(\bar{\psi}^r,j)$, $j = r,r-1,\ldots,\frac{r}{2}$. If one passes to partial L-functions for a suitable integral ideal $\mathfrak{g}$, the special values can be interpreted as special values of non holomorphic Eisensteinseries

$$E(\alpha,\mathfrak{g}) = \sum \frac{(\overline{\alpha+\omega})^{r-j}}{(\alpha+\omega)^r}$$

By some classical summation processes which go back to Eisenstein and Kronecker one expresses the non-holomorphic Eisenstein series in terms of the holomorphic ones. Then one can express the L-values $L(\bar{\psi}^r, r)$ in terms of the $L(\bar{\psi}^{\nu},1)$ for $\nu = 1,\ldots,r$. The "holomorphic" L-values $L(\bar{\psi})$ are expressed in terms of the elliptic modular functions and the period. For our particular character we get

$$(2\pi i)^{r-j} \frac{L(\bar{\psi}^r,j)}{\Omega^r} \in k\ .$$

N. SCHAPPACHER:

On p-adic L-functions

In the first part of the talk, a parallel outline was given of the construction of the types of p-adic L-functions based on interpo-

lating complex zeta - or L- values:
1. the Kubota-Leopoldt p-adic zeta-function of a totally real number field.
2. the "one variable p-adic L-function" of an elliptic curve E/k with complex multiplication by the ring of integers of the imaginary quadratic field k .
3. The "two variable p-adic L-function" of E/k .

To state the results in the cases 2. and 3. , let $p \neq 2,3$ be a rational prime that splits in K : $(p) = \mathfrak{p}\mathfrak{p}^*$ so that E has a good reduction mod $\mathfrak{p}$ and $\mathfrak{p}^*$; ψ, $\bar{\psi}$ the complex Hecke characters of E/k ; $\psi_{\mathfrak{p}}$, $\psi_{\mathfrak{p}}^*$: $G(k^{ab}/k) \to \mathbb{Z}_p^*$ their p-adic analogues, giving the Galois action on $E_{\mathfrak{p}^\infty}$, $i_{\mathfrak{p}} : k^{ab} \to \mathbb{C}_p$ inducing $\mathfrak{p}$ on k ; J the valuationring of the completion of $k(E_{\mathfrak{p}^\infty})$; $\Omega_\infty \in \mathbb{C}^*$, $\Omega_{\mathfrak{p}} \in J^*$ the complex and p-adic period of E .
1-variable theorem: Let $\mathfrak{g} \subset \mathfrak{o}_k$ be an ideal $\neq (0), (1)$, $\mathfrak{p} \nmid \mathfrak{g}$. There is a unique measure $\mu_{\mathfrak{g}} \in J[[G(k(E_{\mathfrak{p}^\infty})/k)]]$ such that: for all $r \geq 1$ with $\mathrm{cond}(\psi^r) \mid \mathfrak{g}$ one has

$$i_{\mathfrak{p}}^{-1}\left(\frac{\psi^r(\mu_{\mathfrak{g}})}{\Omega_{\mathfrak{p}}^r}\right) = A(0,r)\ \frac{L_{\mathfrak{g}}(\psi^r,1)}{\Omega_\infty}\left(1 - \frac{\psi^r(\mathfrak{p})}{\mathbb{N}\mathfrak{p}}\right) ,$$

where $L_{\mathfrak{g}}$ is the usual Euler product with factors removed in the primes dividing $\mathfrak{g}$.

2-variable theorem: Let $\mathfrak{g}$ be like above. There is a unique measure $\nu_{\mathfrak{g}} \in J[[\,G(k(E_{p^\infty})/k]]$ such that:
for all $r > -j \geq 0$ with $\mathrm{cond}(\psi^{r-j}) \mid \mathfrak{g}$,

$$i_{\mathfrak{p}}^{-1}\left(\frac{\psi_{\mathfrak{p}}^r\,\psi_{\mathfrak{p}^*}^j(\nu)}{\Omega^{r-j}}\right) = A(j,r)\ \frac{L_{\mathfrak{g}}(\psi^r\bar{\psi}^j,1)}{\Omega_\infty^{r-j}}\left(1 - \frac{\psi^r\bar{\psi}^j(\mathfrak{p})}{\mathbb{N}\mathfrak{p}}\right)\left(1 - \frac{(\check{\psi^r}\bar{\psi}^j)(\mathfrak{p})}{\mathbb{N}\mathfrak{p}}\right) .$$

Here, $\check{\rho}(\mathfrak{r}) = \frac{\mathbb{N}\mathfrak{r}}{\rho(\mathfrak{r})}$, for any Hecke character;

$$A(j,r) = \frac{\omega(-j)(2\pi i)^{r-1}}{\sqrt{d_k}^{k-1}}\ \sqrt{\mathbb{N}\ \mathrm{cond}\ \psi^{k-j}}^{1-k-j}\ (\Gamma(1-j)) .$$

Finally, a version of Mazur Swinnerton-Dyer L-functions for modular curves was sketched.

References: J. Coates - A. Wiles: J. Australian Math. Soc. (Ser. A) 26, (1978), 1-25

Katz: Ann. of Math. 104, (1976), 459-571,
Katz: Inventions 49 (1978), 199-297,
J.P. Serre: CR. Acad. Sc. Paris, t 287 (1978), Ser. A, 183-188,
G. Stevens: Arithmetic on Modular Curves, Birkhäuser - green series (1982),
R. Yager: Ann. of Math. 115 (1982), 419-449.

J. COATES:

Remarks on the main conjectures for elliptic curves with complex multiplication

The fundamental difficulty of the arithmetic of elliptic curves is to link the arithmetic invariants of the curve (its Mordell-Weil group and its Tate-Šafarevič group) with the behaviour of its Hasse-Weil L-series at the point $s = 1$. Iwasawa theory gives a means of attaching this problem by p-adic techniques, via the so called main conjectures, which, roughly speaking, affirm that the characteristic power series of the Iwasawa modules which arise from the theory of infinite descent on the curve are none other than the p-adic L-functions which arise by the interpolation of special values of complex L-functions attached to the curve. A precise formulation of these main conjectures was given for elliptic curves with complex multiplication (to avoid technical complications the elliptic curve was assumed to be defined over the field of complex multiplications). A brief discussion was given of the weak results we know in the direction of these main conjecture at present. It was also shown how R. Greenberg has derived the following result from one of these weak versions of the main conjecture.

Theorem (R. Greenberg) Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication. If the Hasse-Weil L-series of E has a zero of odd multiplicity at $s = 1$, then either $E(\mathbb{Q})$ is infinite or the Tate-Šafarevič group of E is enormous in the sense that it contains $\bigoplus_{p \text{ ordinary}} \mathbb{Q}_p/\mathbb{Z}_p$, where the sum is taken over the primes p, ordinary for E (except perhaps 2, 3).

D. HUSEMÖLLER:

David Rohrlich's work on $L(1,\chi)$ and $L'(1,\chi)$

Let K be an imaginary quadratic field of classnumber 1 and let P be a finite set of rational primes. Form the maximal anticyclotomic extension L of K unramified outside P. Note: $\prod_{p\in P} \mathbb{Z}_p \cong$ subgroup of $G(L/\mathbb{Q})$ of finite index.

Let E be an elliptic curve over $\mathbb{Q}$ with a CM action by $\mathcal{O}_K$ in K. Let $V = \mathbb{C} \otimes_{\mathcal{O}_K} E(L)$ with $G(L/K)$-action and decompose

$$V = \bigoplus_{\rho\in \mathrm{Hom}(G(L/K),\mathbb{C}^*)} V(\rho) .$$

$V(\rho)$ is the subspace where $G(L/K)$ acts via the character ρ. The L-series of $E/\mathbb{Q}$, E/K are $L(E/\mathbb{Q},s) = L(\phi,s)$, $L(E/K,s) = L(\phi,s)L(\bar{\phi},s)$. Consider the set $X = \{(\rho\circ \mathrm{Artin})\phi : \rho \in \mathrm{Hom}(G(L/K),\mathbb{C}^*)\}$ of all "anticyclotomic" twists of ϕ. For $\chi \in X$: $\Lambda(\chi,s) = w(\chi)\,\Lambda(\chi,2-s)$.

Main theorem: For all but a finite number of χ we have

$$\mathrm{ord}_{s=1} L(\chi,1) = \begin{cases} 0 & \text{if } w(\chi) = +1 \\ 1 & \text{if } w(\chi) = -1 \end{cases}$$

or in other words $L(\chi,1) \neq 0$ if $w(\chi) = +1$ and $L(\chi,1) = 0$, $L'(\chi,1) \neq 0$ if $w(\chi) = -1$.

J. MESTRE:

Elliptic curves of high rank

Si E est une courbe elliptique sur $\mathbb{Q}$, de conducteur N, le groupe de Mordell-Weil de ces points rationnels sur $\mathbb{Q}$ est de type fini; nèanmoins, il est difficile de calculer exactement le rang $E(\mathbb{Q})$. Le majorations de ce rang r étant en général obtenues par des méthodes de descente faisant intervenir l'arithmétique du corps $\mathbb{Q}(E_2)$. D'autre part, on ignore si ce rang est borné ou non

lorsque E parcourt les courbes elliptiques définies sur $\mathbb{Q}$.

Si l'on admet les conjectures du Weil et de Birch et Swinnerton-Dyer, on peut obtenir des majorations de la forme $r = o(\log N)$; cependant, si l'on admet de plus l'hypothèse de Riemann pour la fonction L de E , on obtient $r = o(\log N/\log\log N)$.

De plus, cette méthode permet d'obtenir des courbes elliptiques de rang élevé, en imposant aux courbes d'avoir un nombre de points modulo p aussi élevé que possible. On trouve ainsi une courbe de rang ≥ 12 (égal à 12 si les conjectures déjà citées sont vraies.

D'autre part, le fait que les majorations obtenues sont bonnes provient de ce que les zêros de L autre que 1 sont "assez" éloignés de 1 .

D. BERNADI:

A p-adic Analogue of the Conjecture of Birch and Swinnerton-Dyer

A report of a joint work with C. Goldstein and N. Stephens.
Let E/K be an elliptic curve with complex multiplication by the ring $\mathcal{O}$ of integers in K ; let $p = \mathfrak{p}\bar{\mathfrak{p}}$ be an odd prime not dividing the conductor of E which splits in K . There is a unique function $L_{\mathfrak{p}}$ continous from $\mathbb{Z}_p$ to S_p the ring of integers in the completion of the maximal unramified extension of $\mathbb{Q}_p$ such that

$$\Omega_{\mathfrak{p}}^{-k} L_{\mathfrak{p}}(k) = (k-1)!\left(1 - \frac{\psi^k(\mathfrak{p})}{N\mathfrak{p}}\right)\Omega_\infty^{-k} L(\psi^k, k)$$

for $k \geq 1$, $k \equiv 1 \pmod{p-1}$

Denote by $c_{\mathfrak{p}}$ the dominant coefficient of $L_{\mathfrak{p}}$ at $s = 1$, and by $\langle , \rangle_\infty$ and $\langle , \rangle_{\mathfrak{p}}$ the complex and p-adic height pairing modified as in Gross' conjecture; then we conjecture:

$$\frac{c_{\mathfrak{p}}}{\Omega_{\mathfrak{p}} \det\langle P_i, P_j\rangle_\infty} = \left(1 - \frac{\psi(\mathfrak{p})}{N\mathfrak{p}}\right) \frac{c_\infty}{\Omega_\infty \det\langle P_i, P_j\rangle_{\mathfrak{p}}}$$

O. ZAGIER:

Factorization of singular modular invariants (joint work with B. Gross

As is well known the j-invariant of an elliptic curve with complex multiplication is an algebraic integer in a classfield over the CM field. To be specific, let $p \equiv 3 \pmod 4$ be prime $j = j(\frac{1+i\sqrt{p}}{2})$. Then j lies in the real subfield H_0 of the Hilbert classfield H of $K = \mathbb{Q}(\sqrt{-p})$; indeed it is known that $j^{1/3}$ and $((j-1728)^{1/2}/\sqrt{-p})$ belong to H_0. The striking thing is that these numbers are highly factored. Berwick (Proc. London Math. Soc. 1928!) noticed empirically that if we write $N_{H_0/\mathbb{Q}}(j) = a^3$, $N_{H_0/\mathbb{Q}}(j-1728) = -b^2p$, then all prime factors of a or b are $<p$ and quadratic non-residues mod p. (Example: for $p = 907$, he found $a = 2^{19} \cdot 3^3 \cdot 5^3 \cdot 131 \cdot 137 \cdot 161$, $b = 2^9 \cdot 3^9 \cdot 7^6 \cdot 11^6 \cdot 47 \cdot 67^2 \cdot 79 \cdot 331$) This follows from

Theorem: Let l be a prime. Then $l|a \iff 3p = x^2 + 4lN\mathfrak{a}$ for some (odd) integer $x > 0$ and integral ideal $\mathfrak{a}$ of K, and similary $l|b \iff p = x^2 + lN\mathfrak{a}$. Moreover, the power of l in a or b is the number of such representations, counted with multiplicity $e + 1$ if $l^e \| \mathfrak{a}$.

Similar results also hold for the discriminant of the minimal polynomial of j (for instance, for $p = 71$ with $h(-p) = 7$ the polynomial of j is

$j^7+313645809715j^6 +...+ 7377070867607311133577142410060812 63$

with discriminant

$-7^{84} \cdot 11^{42} \cdot 13^{42} \cdot 17^{26} \cdot 31^{12} \cdot 41^6 \cdot 47^6 \cdot 53^4 \cdot 59^6 \cdot 61^4 \cdot 67^2 \cdot 71^3$

an example mentioned in a recent paper of Jensen and Yui in J.N.T.) and for the differences of j-values of different elliptic curves with CM (even by different quadratic fields). Two proofs were discussed. One, an algebraic one, actually gives the prime factorization of j and $j - 1728$ in H_0, rather than just their norms. The other method is analytic: one restricts to the diagonal a non-holomorphic Hilbert Eisenstein series of weight 1 which vanishes at $s = 0$, computes the s-derivative at $s = 0$ and projects the

resulting modular form of weight 2 onto its modular part; the result must be 0 (since there are no holomorphic cuspforms of weight 2 on $SL_2(\mathbb{Z})$) and the formula for the Fourier coefficients gives the desired identity.

J.W. CASSELS:

Finding rational points on elliptic curves

The lecture commenced with an exposition of the traditional method of finding rational points on abelian varieties of dimension 1 (= elliptic curves with given rational point). As an illustration the author reported on joint work with A. Brenner on the curves $y^2 = x(x^2 + p)$ where p is prime, $p \equiv 5 \pmod 8$. The Selmer conjecture (as also the Birch-Swinnerton-Dyer conjectures) predicts rank = 1 . The case $p = 877$ was described in some detail and it was shown that the rational points on $y^2 = x(x^2 + 877)$ are generated by $(0,0)$ and (x_0, y_0) , where

$$x_0 = \frac{3754945281271621931055040699420927923462 01}{6215987776871505425463220780697238044100}$$

$$y_0 = \frac{256\ 2562\ 6798\ 8926\ 8093\ 8877\ 6834\ 0455\ 1308\ 9648\ 6691\ 5320\ 4356\ 6034\ 6478\ 6949}{4900\ 7802\ 3219\ 7875\ 8895\ 9802\ 9339\ 9592\ 8925\ 0960\ 6161\ 6470\ 7799\ 7926\ 1000}$$

B.J. BIRCH:

Calculation of Heegner points of elliptic curves

Suppose that E is a Weil curve of conductor N , so we may parametrize E by functions $x(z), y(z) \in \mathbb{Q}(j(z), j(Nz))$. If $R = \mathbb{Z}\left[\frac{\Delta + \sqrt{\Delta}}{2}\right]$ is a complex quadratic ring in which every prime ideal dividing N splits, so that $N = \mathfrak{n}\bar{\mathfrak{n}}$, it is sensible to talk about $j(\mathfrak{a})$ when $\mathfrak{a}$ is an ideal of R . We say $P(\mathfrak{a},\mathfrak{n}) := (j(\mathfrak{a}), j(\mathfrak{n}\mathfrak{a}))$ is a Heegner point of $X_0(N)$, if $\mathfrak{a}$ and $\mathfrak{n}\mathfrak{a}$ are both primitive ideals of R . Suppose now $\Delta = ef$, where e,f discriminants of quadratic fields, let χ_e, χ_f be the corresponding quadratic character, and let $\psi(\mathfrak{a}) = \chi_e(\mathfrak{a}\bar{\mathfrak{a}})\, \chi_f(\mathfrak{a}\bar{\mathfrak{a}})$ be the genus character. The point $\sum_{\text{classes}\,\mathfrak{a}} \psi(\mathfrak{a})\, P(\mathfrak{a},\mathfrak{n})$ of $E(\mathbb{Q}(\sqrt{e},\sqrt{f}))$ gives a

rational point $P_{e,f}$ either of the twist $E^{(e)}$ or of $E^{(f)}$. Suppose that $P_{e,f} \in E^{(e)}(\mathbb{Q})$.

The construction of P_{e,fm^2} in fact makes sense whenever ① e,f are field discriminants such that every prime factor of N splits or ramifies in $\mathbb{Q}(\sqrt{ef})$ and ② there are no primes p such that <u>either</u> $p^2|N$ and $p|efm^2$ <u>or</u> $p|N$ and $p^2|efm^2$. Computations of Stephens and Birch suggested the <u>conjecture</u> that (apart for a few cases with $(ef,N) = 1$ in which $P_{e,f}$ is trivial for trivial reasons) the canonical height of $P_{e,f}$ is, up to a power of 2, equal to $L'(E^{(e)},1)L(E^{(f)},1)/\Omega_e\Omega_f$ where Ω_e, Ω_f are the real periods; and this is in process of becoming a theorem in the triumphant hatch of Gross and Zagier.

Restrict now to the case where $E^{(e)}(\mathbb{Q})$ has rank 1 and $L'(E^{(e)},1) \neq 0$; fix a generator P_e of $E^{(e)}(\mathbb{Q})$ for each such e, and write $P_{e,f} = n(e,f)P_e$. Computations also suggest that $n(e,f)$ is consistent, in the sense that $n(e_1,f_1)n(e_2,f_2) = n(e_1,f_2)n(e_2,f_1)$ - and this too appears to be with in the power of Gross and Zagier. Finally, it is relatively easy to show that $n(e,fm^2)/n(e,f)$ is predictable, and that (for fixed E) the points of $n(e,f)P_e$ depend on $e \cdot f$.

N. STEPHENS:

In certain cases, Heegner points provide a practical method for determining a rational point on an elliptic curve $E/\mathbb{Q}$ as an alternative to the classical method of descent. The basis of the method is to choose a certain complex quadratic extension $K/\mathbb{Q}$ with field discriminant Δ and construct $P_{1,\Delta}$ defined above. By the theorem of Gross and Zagier and the conjectures of Birch and Swinnerton-Dyer the method will be succesful if and only if $E(\mathbb{Q})$ has rank 1 and $E^{(\Delta)}(\mathbb{Q})$ has rank 0. We wish to determine $E(\mathbb{Q})$; for simplicity, we shall assume that E is a Weil curve, although this is not always necessary. The steps in the method are as follows.

1. Determine the torsion subgroup of $E(\mathbb{Q})$.

2. Search for small rational solutions.

3. Compute the conductor N , see Antwerpen IV.

4. Compute ε the sign in the functional equation. If $\varepsilon = -1$ stop (the method will not work).

5. Compute a_n, $n = 1,2,\ldots,CN$, the coefficients of the differential $f(z)dz$.

6. Compute the periods of the lattice.

7. Compute the first 10 coefficients of the series $p(t) = \frac{1}{t^2} + r_0 + r_2 t^2 + \ldots$

8 Choose a complex quadratic field K in which all prime factors of N split, preferably with small class number.

9. Determine $\omega_1,\ldots,\omega_k$ corresponding to the h ideal classes.

10. Determine $u(\omega_i)$, $i = 1,\ldots,h$ where $u(z) = -2\pi i \int_0^{i\infty} f(z)dz \doteq \sum_{n=1}^{CN} \frac{a_n}{n} e^{2\pi i n z}$ (correct to about C decimal places) and determine $U = \sum_{i=1}^{h} u(\omega_i)$.

11. Check that U is not elliptic parameter of torsion point within accuracy. If it is goto 8 with different K . But if it is in the 3^{rd} or 4^{th} time suspect that rank $(E(\mathbb{Q})) \geq 3$ and stop.

12. Compute $\tilde{x} = p(U)$

13. If $P_{1,\Delta} = (x,y)$, $\tilde{x} \doteq x = X/Z^2$ with $X,Z \in \mathbb{Z}$. Use continued fraction algorithm on $\tilde{x}$ to find X,Z . It should be sucessful if $|X Z^2| < 10^C$.

Berichterstatter: V. Diekert

Tagungsteilnehmer

Herrn
Prof. D. Bernardi
Université de Paris VI
Mathématiques
Tour 45-55, Place Jussieu
Paris V^{e}

Frankreich

Herrn
Prof. J.W.S. Cassels
University of Cambridge
Departm. of Pure Math.
16 Mill Lane
Cambridge CB2 1SB

Großbritannien

Herrn
Prof. B.J. Birch
University of Oxford
Math. Inst.
24-29 St. Giles
Oxford

England

Herrn
Prof. J. Coates
Université de Paris Sud
Dpt. de Mathématiques
Bât. 425
91405 Orsay Cédex

Frankreich

Frau
Dr. Gudrun Brattström
Univ. de Paris-Sud
Mathématiques
Bâtiment 425
Centre d'Orsay
91405 Orsay Cédex

Frankreich

Herrn
Volker Diekert
Universität Hamburg
Mathematisches Seminar
Bundesstr. 55

2000 Hamburg 13

Herrn
Dr. J. Brinkhuis
Erasmus University
Dep. of Math. H 7-11
Economic Faculty
3000 DR Rotterdam

Niederlande

Herrn
Dr. C. Deninger
Universität Köln
Mathematisches Institut
Weyertal 86-90

5000 Köln 41

Herrn
Prof. Bushnell
University of London
King's College
Departm. of Mathematics
Strand London WC2R 2LS

Großbritannien

Herrn
Prof. M. Eichler
27, Im Lee
4144 Arlesheim

Schweiz

Herrn
Dr. Everest
University of London
King's College
Departm. of Mathematics
Strand London WC2R 2LS

Großbritannien

Herrn
Prof. R. Gillard
Université de Grenoble
Mathématiques
Saint Martin d'Hères
Grenoble

Frankreich

Herrn
Prof. Dr. G. Frey
Universität Saarbrücken
Fachbereich Mathematik
Bau 27

6600 Saarbrücken

Frau
Dr. Catherine Goldstein
Univ. de Paris-Sud
Mathématique
Bâtiment 425
Centre d'Orsay
91405 Orsay Cédex

Frankreich

Herrn
Prof. A. Fröhlich
Imperial College
Huxley Building, Queens Gate
London SW7 2BZ

Großbritannien

Herrn
Prof. Dr. F. Grunewald
Universität Bonn
Mathematisches Institut
Wegelerstr. 10

5300 Bonn

Herrn
Dr. Ernst Gekeler
Universität Bonn
Mathematisches Institut
Wegelerstr. 10

5300 Bonn

Herrn
Prof. Dr. G. Harder
Universität Bonn
Mathematisches Institut
Wegelerstr. 10

5300 Bonn

Herrn
Prof. Dr. W.-D. Geyer
Universität Erlangen
Mathematisches Institut
Bismarckstr. 1 1/2

8520 Erlangen

Herrn
Dr. D. Husemöller
Haverford College
Dept. of Mathematics
Haverford, P.A. 19041

USA

Herrn
Dr. U. Jannsen
Universität Regensburg
Fachbereich Mathematik
Universitätsstr. 31

8400 Regensburg

Herrn
Dr. W. Kohnen
Max Planck Institut
für Mathematik
Gottfried-Claren-Str. 3

5300 Bonn-Beuel

Herrn
Prof. Dr. W. Jehne
Universität Köln
Mathematisches Institut
Weyertal 86-90

5000 Köln 41

Herrn
Dr. M. Laska
Universität Bonn
Mathematisches Institut
Wegelerstr. 10

5300 Bonn

Herrn
Dr. E. Kani
Universität Heidelberg
Mathematisches Institut
Im Neuenheimer Feld 288

6900 Heidelberg

Herrn
Prof. H.W. Lenstra Jr.
Mathematisch Instituut
Roetersstraat 15
Amsterdam

Niederlande

Herrn
Dr. N. Klingen
Universität Köln
Mathematisches Institut
Weyertal 86-90

5000 Köln 41

Herrn
Prof. S. Lichtenbaum
Univ. de Paris-Sud
Mathematique
Bâtiment 425
Centre d'Orsay
91405 Orsay Cédex

Frankreich

Herrn
Prof. Dr. M. Kneser
Universität Göttingen
Mathematisches Institut
Bunsenstr. 3-5

3400 Göttingen

Herrn
Dr. B.H. Matzat
Universität Karlsruhe
Math. Inst. II
Englerstr. 2

7500 Karlsruhe

Herrn
Dr. J. Mestre
University of Bordeaux
Mathematics Department
Bordeaux

Frankreich

Herrn
Prof. Olsen
Dept. of Mathematicx
University of Tromsø
Postboks 953
9001 Tromsø

Norwegen

Herrn
Prof. A. Néron
Univ. de Paris-Sud
Mathematique
Bâtiment 425
Centre d'Orsay
91405 Orsay Cédex

Frankreich

Herrn
Dr. B. Perrin-Riou
Université de Paris VI
Mathématiques
Tour 45-55
Place Jussieu
Paris V^{e}

Frankreich

Herrn
Prof. Dr. J. Neukirch
Univ. Regensburg
Fachbereich Mathematik
Universitätsstr. 31

8400 Regensburg

Herrn
Prof. Dr. M. Rapoport
Universität Heidelberg
Mathematisches Institut
Im Neuenheimer Feld 288

6900 Heidelberg

Herrn
Prof. J. Oesterlé
Ecole Normale Sup. Paris
45 rue d'Ulm
75005 Paris

Frankreich

Herrn
Prof. Dr. J. Ritter
Lehrstuhl für Reine Mathematik
Universität Augsburg
Memmingerstr. 6

8900 Augsburg

Herrn
Prof. A.P. Ogg
Max Planck Institut
für Mathematik
Gottfried-Claren-Str. 3

5300 Bonn

Herrn
Prof. G. Robert
Université de Grenoble
Dept. de Mathématiques
Saint Martin d'Hères
38000 Grenoble

Frankreich

Herrn
Prof. Dr. P. Roquette
Universität Heidelberg
Mathematisches Institut
Im Neuenheimer Feld 288

6900 Heidelberg

Herrn
Dr. P. Satgé
Université de Caen
Dept. de Mathématiques
14032 Caen Cédex

Frankreich

Herrn
Dr. Schappacher
Universität Göttingen
Mathematisches Institut
Bunsenstr. 3-5

3400 Göttingen

Herrn
Dr. C. Schmidt
Universität Saarbrücken
Fachbereich Mathematik
Bau 27

6600 Saarbrücken

Herrn
Dr. P. Schneider
Universität Regensburg
Fachbereich Mathematik
Universitätsstr. 31

8400 Regensburg

Herrn
Prof. J. Tate
Dept. Mathematics
Harvard University
Science Center
1 Oxford St.
Cambridge, Mass.

USA

Herrn
Dr. M. Taylor
Trinity College
Cambridge CB2 1SB

Großbritannien

Herrn
Dr. R.J. Schoof
Rijksuniversiteit Leiden
Mathematisch Instituut
Wassenaarseweg 80
2333 AL Leiden

Niederlande

Herrn
Dr. J. Schwermer
Universität Bonn
Mathematisches Institut
Wegelerstr. 10

5300 Bonn

Herrn
Dr. N. Stephens
Univ. de Paris-Sud
Mathematique
Bâtiment 425
Centre d'Orsay
91405 Orsay Cédex

Frankreich

Herrn
Dr. J. Tilouine
Univ. de Paris-Sud
Mathematique
Bâtiment 425
Centre d'Orsay
91405 Orsay Cédex

Frankreich

Herrn
Dr. Jing Yu
Université de Paris-Sud
Mathématiques
Bâtiment 425
91405 Orsay

Frankreich

Herrn
Dr. St. Wilson
Science Laboratory
Dept. of Mathematicx
Southroad
Durham DH1 1SZ

Großbritannien

Herrn
Prof. Dr. D. Zagier
Universität Bonn
Mathematisches Institut
Wegelerstr. 10

5300 Bonn

Herrn
Dr. K. Wingberg
Universität Regensburg
Fachbereich Mathematik
Universitätsstr. 31

8400 Regensburg

Herrn
Prof. Dr. H.G. Zimmer
Universität Saarbrücken
Fachbereich Mathematik
Bau 27

6600 Saarbrücken