Mathematisches Forschungsinstitut Oberwolfach

Report No. 32/2003

Explicit Methods in Number Theory

July 20th – July 26th, 2003

The conference was organized by H. Cohen (Talence) H.W. Lenstra (Leiden) and D. Zagier (Bonn, Utrecht).

The goal was to present new methods and results on concrete aspects of number theory. In many cases this included computational and experimental work, but with the primary emphasis being on the implications for number theory rather than on the computational methods used.

A 'mini-series' of three 1-hour lectures was given by Manjul Bhargava about the parametrisation of algebraic structures. Two 1-hour lectures were given by Yuri Bilu about the work of Preda Mihailescu on the Catalan equation.

Some of the other main themes included:

- rational points on curves and higher dimensional varieties
- class number formulas, Stark's conjecture, algebraic K-theory
- analytic algebraic number theory
- Diophantine equations

As always in Oberwolfach, the atmosphere was ideal for exchanging ideas and conducting lively discussions.

Abstracts

Construction of irreducible polynomials over prime finite field of large characteristic

Bill Allombert

Given a prime number p and an integer n, we want to compute an irreducible polynomial of degree n over $\mathbb{F}_p$.

The first deterministic polynomial time algorithm (under the Extended Riemann Hypothesis) solving this question was given in 1986 by Adleman and Lenstra, using polynomials defining subextensions of cyclotomic fields.

We present a modification of this algorithm that computes the defining polynomial over $\mathbb{Q}_\ell$ for some well-chosen prime ℓ instead of computing it in an $\mathbb{F}_p$-algebra. This approach leads to a faster algorithm than the original, which is more efficient in practice than the other known algorithms when p is large, although still having a deterministic polynomial running time under the ERH.

Factoring polynomials using van Hoeij's method

Karim Belabas

Mark van Hoeij proposed an algorithm for factoring polynomials over the rational integers, which rests on the same principle as Berlekamp-Zassenhaus (compute factor bound, choose prime p and factor over $\mathbb{Q}_p$, then recombine modular factors) but uses lattice basis reduction to improve drastically on the recombination phase. His ideas give rise to a collection of algorithms, differing greatly in their performance characteristics. We present a deterministic variant which achieves good overall performance (experimentally), and can be proven to terminate in finite time. I conjecture it is actually polynomial time. This variant was generalized to number field, and is typically able to factor polynomials with hundreds of modular factors in a few minutes, even when they have few rational factors.

Catalan without Tijdeman

Yuri Bilu

I spoke on the new work of Preda Mihailescu, who used the argument of Bugeaud and Hanrot to prove that in Catalan's equation $x^p - y^q = 1$, none of the exponents is 1 mod the other. This is an important step in Mihailescu's celebrated proof of Catalan's conjecture; before this new development, it could be done only using logarithmic forms and extensive electronic computations. Now the proof of Catalan is totally independent of logarithmic forms and computers.

Ranks of quadratic twists of an elliptic curve

Dongho Byeon

Let E be the elliptic curve 37C in Cremona's table with the equation E: $y^2 + y = x^3 + x^2 - 23x - 50$. In this talk I will show that for at least 40 percent. of the positive fundamental discriminants D and at least 24 percent. of the negative fundamental discriminants D, $Ord_{s=1}L(s, E_D) = 1$.

Parity of modular degrees

F. Calegari

Let E be a (modular) elliptic curve of conductor N. There exists a minimal modular parametrization:

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

The degree $\deg(\pi)$ is called the *modular degree*. Suppose that the conductor of E is prime, and that the modular degree of E is odd. Then we show that N is 3 modulo 8, proving a conjecture of Watkins. Furthermore, we show in such cases that E has supersingular reduction at 2, and that the (Mordell–Weil) rank of $E(\mathbb{Q})$ is zero.

Global obstructions for the descent of coverings and varieties

Jean-Marc Couveignes

We recall what is a field of definition and a field of moduli. We show that there exist global obstructions for the field of moduli to be a field of definition.

Let $\mathbb{Q}$ be the field of rationals.

Theorem : there exists a projective regular irreducible variety over $\bar{\mathbb{Q}}$ having $\mathbb{Q}$ as field of moduli and admitting a model over any completion of $\mathbb{Q}$ but no model over $\mathbb{Q}$.

So the local-global principal fails for descent of varieties. It also fails for coverings (as we also prove).

Our proof builds on classical examples from class field theory and inverse Galois techniques, plus some natural geometric constructions.

Local obstructions for the existence of a model over the field of definition were known to exist for varieties (Mestre) and for coverings (Couveignes).

Very explicit descent on elliptic curves

John Cremona and Michael Stoll
(joint work with T. A. Fisher (Cambridge), C. O'Neil (MIT), D. Simon (Caen))

Let E/K be an elliptic curve over a number field. Descent on E attempts to get information on both the Mordell-Weil group $E(K)$ and the Shafarevich-Tate group $Ш(E/K)$. For each $n \geq 2$, there is an exact sequence

$$0 \longrightarrow E(K)/nE(K) \longrightarrow \mathrm{Sel}^{(n)}(E/K) \longrightarrow Ш(E/K)[n] \longrightarrow 0\,,$$

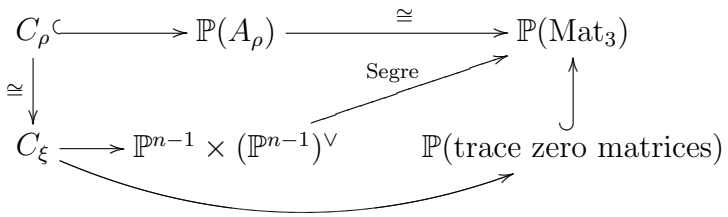
where $\mathrm{Sel}^{(n)}(E/K)$ is the n-Selmer group. Our goal is to compute the n-Selmer group, and represent its elements explicitly as curves $C \subset \mathbb{P}^{n-1}$ (when $n \geq 3$). Having this representation allows searching for points on C (which in turn give points in $E(K)$, since C may be seen as an n-covering of E), and also doing higher descents.

Let $A = \mathrm{Map}_K(E[n], \overline{K})$ be the affine algebra of the scheme $E[n]$. There is an isomorphism $H^1(K, E[n]) \xrightarrow{\sim} H$, where H is a subquotient of $(\mathrm{Sym}^2 A)^\times$; for n prime, we also have $H \hookrightarrow A^\times/(A^\times)^n$ (Shaefer, Stoll). This can be used to find the image of $\mathrm{Sel}^{(n)}(E/K)$ in H.

Let $\xi \in H$ be represented by $\rho \in (\mathrm{Sym}^2 A)^\times$. The

curve C_ξ corresponding to ξ can be embedded in S_ξ, a twist of $\mathbb{P}^{n-1}$ (a Brauer-Severi variety). For ξ in the Selmer group we have $S_\xi \cong \mathbb{P}^{n-1}$. In order to obtain $C_\xi \subset \mathbb{P}^{n-1}$

we represent the obstruction against $S_\xi \cong \mathbb{P}^{n-1}$ as a central simple algebra A_ρ over K (constructed from ρ and A) and then find an explicit isomorphism $A_\rho \cong \mathrm{Mat}_n(K)$. We can always find a model $C_\rho \subset \mathbb{P}(A_\rho)$; using this isomorphism, we have a diagram



Projection onto the first factor $\mathbb{P}^{n-1}$ gives $C_\xi \subset \mathbb{P}^{n-1}$. This has been implemented for $K = \mathbb{Q}$ and $n = 3$.

Computations with L-functions of curves

T. Dokchitser

There are various conjectures concerning ζ- and L-functions of arithmetic origin. These functions are supposed to possess meromorphic continuation to the complex plane, satisfy a predicted functional equation and Riemann hypothesis. Also, there are numerous conjectures concerning special values at integer points, for instance the conjectures of Birch-Swinnerton-Dyer, Stark, Deligne-Scholl-Beilinson, Lichtenbaum and Bloch-Kato. This talk is aimed to explain how to test these conjectures for higher genus curves. One aspect of this is essentially analytic, the actual computation of values of L-series. Another one is arithmetic, understanding the invariants which enter the functional equation. One illustration of the latter is how to determine local factors of L-series of higher genus curves at primes of bad reduction.

Computation of fields of definition of torsion points of Jacobian varieties.

Bas Edixhoven

The aim of the talk is to explain my strategy to compute fields of definition of torsion points of jacobian varieties, and to give an account of what has already been done.

To give the idea, an example concerning the 5-torsion of an elliptic curve E in Weierstrass form is given. One takes a nonzero differential form ω considers the map:

$$E(\mathbf{C}) \to \mathbf{C}/\Lambda, \quad P \mapsto \int_\infty^P \omega$$

For a given 5-torsion point x in $\mathbf{C}/\Lambda$, there is a unique P that is mapped to x. To approximate this P, one uses Newton's method and formal integration of power series. The approximation then gives the minimal polynomial of the coordinates of P. Let K be a number field, O_K its ring of integers. Let X be an arithmetic surface over the spectrum S of the ring O_K, assumed to be semistable. Let $\pi\colon X \to S$ denote the structure map, and suppose that we have a section P. Suppose that D and D' are effective horizontal divisors on X, such that $D' - D$ is torsion on the generic fibre. Put $E := P^* O_X(D' - D)$, equipped with its metrics at the infinite places from Arakelov theory. Then, using arithmetic Faltings's Grothendieck Riemann Roch, plus Noether's formula (Moret-Bailly), one gets an estimate:

$$\deg(E) \leq -\frac{1}{2}\langle D + V, D + V - \omega\rangle + h(X) + \sum_\sigma \log \|\theta\|_{\sigma,\sup} + \frac{g}{2}[K : \mathbf{Q}] \log(2\pi).$$

This estimate was obtained in collaboration with Robin de Jong (Amsterdam). It should suffice to bound the required precision for the approximation part.

As a possible application I think of the 2-dimensional subspace V_l of $J_1(l)(\overline{\mathbf{Q}})[l]$ that corresponds to the modular

form Δ of weight 12. For $X = X_1(l)$ it seems that the terms in the estimate above are polynomial in l (but we are not so sure yet about $\log \|\theta\|_{\sigma,\sup}$). *If* the estimates will indeed turn out to be polynomial in l, and *if* the approximation (with the required precision)can be done in time polynomial in l, *then* we get an algorithm to compute V_l in time polynomial in l, and an algorithm to compute $\tau(p)$ in time polynomial in $\log p$ (as in Schoof's algorithm).

Effective methods for the computation of the cohomology of arithmetic groups and application to the K-theory of the integers.

Philippe Elbaz-Vincent

(joint work with Herbert Gangl(MPI Bonn) and Christophe Soulé (CNRS & IHES))

We will explain how we can compute reasonably efficiently the cohomology of $GL_N(Z)$ or $SL_N(Z)$, with $N < 8$, using the theory of perfect forms developed initially by Voronoi, and in particular the equivariant spectral sequence associated to the Voronoi complex. From then, we will explain how we can deduce, modulo some non-trivial homotopical arguments, that $K_5(Z) = Z$ and $K_6(Z) = 0$. We will also mention some related works in progress.

Curves $\mathbf{E_k : X^3 + Y^3 = k}$ of high rank

Noam D. Elkies

(joint work with Nicholas F. Rogers)

r	smallest k such that $E_k : X^3 + Y^3 = k$ has rank r
0	1
1	$6 = 2 \cdot 3$
2	19 (prime)
3	$657 = 3^2\,73$
4	$21691 = 109 \cdot 199$
5	$489489 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 163$
6	$9902523 = 3 \cdot 73 \cdot 103 \cdot 439$ (*)
7	$1144421889 = 3 \cdot 13 \cdot 19 \cdot 41 \cdot 139 \cdot 271$ (*)
8	$\le 1683200989470 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29 \cdot 41 \cdot 47 \cdot 59$ (**)
9	$\le 18686874226924241 = 13 \cdot 23 \cdot 31 \cdot 43 \cdot 61 \cdot 73 \cdot 157 \cdot 199 \cdot 337$

(*) Minimal assuming parity conjecture and GRH for $L(E_k, s)$ ($k < 1144421889$)
(**) Minimality is likely but not proved

In particular we have the first known cases of $r > 7$. For each k, the curve E_k is 3-isogenous with $E'_k : XY(X + Y) = k$, an elliptic curve with a rational 3-torsion point. Thus $E'_k(\mathbb{Q}) \cong \mathbb{Z}^9 \oplus (\mathbb{Z}/3\mathbb{Z})$ for $k = 18686874226924241$. The previous rank record for *any* elliptic curve over $\mathbb{Q}$ with a 3-torsion point was 8 [Kulesz-Stahlke 2001, Dujella 2001]. Also new are: the $r = 6$ and $r = 7$ examples, which improve on N.F.Rogers' earlier records; their proofs of conjectural minimality; and (we think) the proofs of minimality for $r = 4, 5$

(Selmer already claimed the $r = 3$ minimum in 1951). The $r = 8$ example also has the curious feature of 8 independent *integer* solutions of $xy(x + y) = k$, namely

$$(x, y) = (11, 391170),\ (533, 55930),\ (770, 46371),\ (1003, 40467),$$
$$(2639, 23970),\ (6970, 12441),\ (7293, 1197),\ (8555, 10387).$$

These yield independent points on $E_k(\mathbb{Q})$.

Let $P_1(X, Y) = X^3 + Y^3$ and $P_2(X, Y) = XY(X + Y)$. We want integers that can be written as the cubefree part $d^{-3}P_1(x, y)$ or $d^{-3}P_2(x, y)$ for many $x, y \in \mathbb{Z} \cap [-H, H]$. But there are some H^2 choices of (x, y), which will clog our CPU and/or memory with k-values most of which have $r = 1$. We reduce this H^2 to H by searching over pairs of points: solutions to $P_i(x, y) = P_j(x', y')$ with $(i, x, y) \neq (j, x', y')$. This is possible because in each case $P_i(x, y) = P_j(x', y')$ is a rational cubic surface. Such a surface is expected to have $CH \log^A(H)$ rational points of height up to H, of which we can find about H in time $C'H \log^B(H)$ by using all $(r : s : t) \in \mathbf{P}^2(\mathbb{Q})$ of height $\ll H^{1/3}$ in a rational parametrization such as

$$(x : y : x' : y') = (r^3 - s^3 : s^3 + t^3 : r^2s - s^2t + t^2r : r^2t - s^2r - t^2s)$$

for $(i, j) = (1, 2)$.

For each k, we compute the Selmer ranks for the isogenies $E_k \leftrightarrow E'_k$, and retain only those k for which the upper bound on r is large enough. (This computation is of course also a key ingredient in verifying that E_k has rank exactly r in the above table, and also that these k are minimal for $r \leq 5$ and conjecturally minimal for $r = 6, 7$.) Those 3-descents require the complete factorization of k. Fortunately the 9th-degree form $k(r, s, t)$ splits into linear and quadratic factors for $(i, j) \neq (1, 1)$. Further heuristic refinements include a Mestre threshold on partial products for $L(E_k, 1)$, and a requirement that k be 1613-smooth [NB $1613 = p_{255}$ considerably exceeds the largest prime factor in the above table].

The pair-of-points idea can be applied in other contexts. Mark Watkins has recently used it to find elliptic curves $E/\mathbb{Q}$ (with no restrictions on the form of E) of ranks 9 and 10 whose conductors and/or discriminants are smaller than previous records; a direct search for $E/\mathbb{Q}$ with many integral points would take about 20–50 times longer to reach these new curves. A search for rank 11 is currently in progress.

The Brauer-Manin Obstruction on Curves

Victor Flynn

When a variety violates the Hasse principle, this can be due to an obstruction known as the Brauer-Manin obstruction. It is an unsolved problem whether all violations of the Hasse principle on curves are due to this obstruction. I shall describe computations in progress which test a wide selection of curves, and tries to test for these examples whether the Brauer-Manin obstruction is the cause of all violations of the Hasse principle. This has involved the development of several new techniques, exploiting the embedding of a curve in its Jacobians via a rational divisor class of degree 1.

Multiple polylogarithms, rooted trees and algebraic cycles

Herbert Gangl

We construct, for a field F and a natural number n, algebraic cycles in Bloch's cubical cycle group of codimension n cycles in $\left(\mathbb{P}^1_F \setminus \{1\}\right)^{2n-1}$ which correspond to weight n multiple polylogarithms. Moreover, we construct out of them a differential graded subalgebra in the Bloch-Kriz cycle DGA. In the process, we are led to introduce two other DGA's which are mapped to the cycle DGA: one of them is built from trees (reminiscent of the Connes-Kreimer renormalization Hopf algebra) and the other one from polygons (closely connected to Goncharov's dihedral Lie algebra).

Convex polytopes, the Ehrhart polynomial, and Hecke operators

Paul E. Gunnells
(joint work with Fernando Rodriguez Villegas)

Let P be a simple convex lattice polytope with vertices in the lattice L. Ehrhart proved that the function $t \mapsto \#(tP \cap L)$, as t ranges over all nonnegative integers, is a polynomial $E(P)$ of degree n with rational coefficients. Formulas for the coefficients of $E(P)$ were given by Khovanskii-Pukhlikov, Brion-Vergne, and Diaz-Robins. In general these formulas involve volumes of the faces of P as well as higher-dimensional Dedekind sums generalizing those considered by Zagier.

Let p be a prime number, and let k be an integer with $1 \leq k \leq n-1$. We define a new polynomial $E_{p,k}(P)$ attached to P as follows. Via the isomorphism $p^{-1}L/L \simeq \mathbb{F}_p^n$, any lattice M satisfying $p^{-1}L \supset M \supset L$ determines a subspace $\bar{M} \subset \mathbb{F}_p^n$. Then we put

$$E_{p,k}(P) = \sum E(P_M),$$

where the sum is taken over all M between $p^{-1}L$ and L with $\dim \bar{M} = k$, and where P_M denotes the polytope P thought of as a lattice polytope with vertices in M. Recall that a polytope is called nonsingular if the associated toric variety is nonsingular.

Theorem Suppose P is nonsingular, and for any polynomial f let $c_l(f)$ be the degree l coefficient. Then there is a polynomial $\nu_{k,l}(T) \in \mathbb{Z}[T]$ such that

$$c_l(E_{p,k}(P))/c_l(E(P)) = \nu_{k,l}(p).$$

Moreover, $\nu_{k,l}(p)$ can be explicitly computed as follows. Let $W \subset \mathbb{F}_p^n$ be a fixed subspace of dimension l. Then

$$\nu_{k,l}(p) = \sum p^{\dim(V \cap W)},$$

where the sum is taken over all subspaces $V \subset \mathbb{F}_p^n$ of dimension k. The proof shows that every term of degree l in the Brion-Vergne formula for $E(P)$ transforms by scaling by $\nu_{k,l}(p)$ when passing to $E_{p,k}(P)$. This implies that the Dedekind sums appearing in the computation of c_l satisfy many identities.

On the asymptotics of number fields with given Galois group

Jürgen Klüners

Let k be a number field, G be a finite permutation group, and

$$Z(k,G;x) := |\{K/k \mid \mathrm{Gal}(K/k) = G, \mathrm{N}(d_{K/k}) \leq x\}|.$$

This number is finite for any given real x. There is a conjecture of Malle which says that for $x \to \infty$ we expect

that

$$Z(k,G;x) \sim c(k,G)x^{a(G)}\log(x)^{b(k,G)},$$

where the constants $a(G)$ and $b(k,G)$ are explicitely given. The full conjecture is true for all abelian groups and some small groups. Recently we have proved that there are good lower and upper bounds for nilpotent groups, i.e. we can show for nilpotent groups G: $Z(k,G;x) = O(x^{a(G)}\log(x)^{d(G)})$, where $a(G)$ is as expected and $d(G)$ may be larger than $b(k,G)$.

In this talk we want to show that for the infinite series of generalized quaternion groups we can prove that the corresponding Dirichlet series have a mereomorphic continuation to the left of the critical point. Therefore we get for $k = \mathbb{Q}$ and G a generalized quaternion group that $Z(\mathbb{Q},G;x) \sim c(G)x^{a(G)}$.

In a second part of our talk we show that there are relations between upper bounds for the class group of number fields and our problem. Assuming a weak version of the Cohen-Lenstra-heuristics we are able to show lower and upper bounds for dihedral groups D_ℓ, where ℓ is prime. Furthermore we show that the failure of the asymptotics conjecture means that the Cohen-Lenstra-conjecture is wrong.

Elliptic curve point counting using $X_0(N)$

David R. Kohel

Let $E/\mathbb{F}_{p^r}$ be an ordinary elliptic curve over a finite field of small characteristic p and degree r over the prime field. Let $R/\mathbb{Z}_p$ be the maximal order in the unramified extension of $\mathbb{Q}_p$ of degree r. We describe a general algorithm for lifting modular invariants of E on $X_0(N)(\mathbb{F}_{p^r})$ to p-adic approximations of their canonical lifts to Heegner points on $X_0(N)(R)$. The determination of the zeta function of E is an application. For $N = 1$ this construction recovers the algorithm of Satoh and for $N = 8$ (with $p = 2$), one obtains an algorithm equivalent to the AGM algorithm of Mestre.

The algorithm involves a precomputed correspondence

$$X_0(pN) \to X_0(N) \times X_0(N),$$

whose image is defined by equations $\Phi(P,Q) = 0$. For $N = p^m$, and $X_0(N)$ of genus zero, we find a model for the curves such that the correspondence takes the form $\Phi(x,y) \equiv x^p - y \bmod p$ in terms of a degree one function $x = f(q)$ and $y = f(q^p)$.

The classical theory of complex multiplication implies that the arithmetic action of the Frobenius automorphism on moduli should preserve the geometric data of p-isogenies between the CM elliptic curves related by the correspondence Φ. The interplay between the Frobenius automorphism and iterative Hensel liftings of the CM invariants gives rise to a rapidly convergent algorithm for lifting a Heegner point (or its Galois orbit) to $X_0(N)(R)$.

The computation of the zeta function of E is completed by precomputation of the action of the pullback of Frobenius isogenies on the fibers of an elliptic surface over $X_0(N)$. The action of Frobenius can be determined generically on the elliptic surface, such that its

specialization to a point on $X_0(N)(R)$ gives the action on the differentials of the canonical lift of E to R. In characteristic zero, one can read off the nonzero scalar action of Frobenius (or its dual) as an element of R to algebraically compute its trace.

Hyperelliptic Curves and Deformations

Alan Lauder

Recently I introduced a method for computing the zeta function of a variety over a finite field based upon the "deformation theory" of Bernard Dwork. I have worked this approach out in full detail for smooth projective hypersurfaces, following essentially the theory of Dwork. In this talk I will sketch how the method may be applied to affine hyperelliptic curves, using a relative version of the cohomology theory of Monsky-Washnitzer.

Elliptic surfaces and Heron triangles

Ronald van Luijk

A heron triangle is a triangle with integral sides and integral area. M. Aassila has proved that there exists an infinite parametrized family of pairs of heron triangles with the same area and the same perimeter. Using elliptic surfaces we will prove a generalization, namely that for every positive integer n, there is an infinite parametrized family of n-tuples of heron triangles, all with the same area and the same perimeter.

Capacity of union of real intervals and heights of points on hyperelliptic curves.

Jean-François Mestre
(joint work with J.-B. Bost (Orsay))

In this talk, we rely the capacity of the union of the real intervals $[a_i, b_i]$, $1 \leq i \leq g+1$ to the archimedean height of $P_+ - P_-$ on the hyperelliptic curve

$$C: \quad y^2 = \prod_{i=1}^{g+1} (x - a_i)(x - b_i),$$

where P_+ and P_- are the two infinite points of C.

In the case of elliptic curve, the archimedean height of a real point $P(x_0, y_0)$ of the elliptic curve E of equation

$$y^2 = (x - a)(x - b)(x - c),$$

a, b, c real, is the logarithm of the capacity of the union of the two real intervals defined par the four real numbers

$$0, (x_0 - a)(x_0 - b), (x_0 - b)(x_0 - c), (x_0 - c)(x_0 - a).$$

We give also a quadratically convergent algorithm to compute the capacity of the union of two intervals (so, because of the previous formulae, a quadratically convergent algorithm to compute the archimedean height of a real point on an real elliptic curve. Each step needs two square roots, and there is no need (in contrast with the usual method with sigma functions) to compute the z of the torus corresponding to the point on the curve.

$\mathbf{x^2 + y^3 = z^7}$

Bjorn Poonen
(joint work with Ed Schaefer and Michael Stoll)

We use a descent argument involving the simple group of order 168 to reduce the problem of finding all integer solutions to $x^2 + y^3 = z^7$ with $\gcd(x, y, z) = 1$ to the problem of determining the rational points (satisfying certain congruence conditions) on 10 twists of the Klein quartic curve

$$X\colon x^3y + y^3z + z^3x = 0$$

in $\mathbb{P}^2$. The relevant twists were determined by a combination of methods, one of which involved identifying X with the modular curve $X(7)$ and using the modularity of elliptic curves over $\mathbb{Q}$. For 9 of the 10 curves, our list of rational points satisfying the congruence conditions has been proved complete by variants of Chabauty's method. If, as is likely, our list for the 10-th curve also is complete, then the original equation has exactly 16 solutions, namely

$$(\pm 1, -1, 0), \quad (\pm 1, 0, 1), \quad \pm(0, 1, 1), \quad (\pm 3, -2, 1), \quad (\pm 71, -17, 2),$$
$$(\pm 2213459, 1414, 65), \quad (\pm 15312283, 9262, 113), \quad (\pm 21063928, -76271, 17)\,.$$

L-functions and random matrix theory

M. Rubinstein

We present a precise conjecture for moments of general families of zeta- and L-functions on or near the critical line or at or near the central critical point which includes the full asymptotic expansion in the case of integral moments and as many finite terms as we desire for non-integer moments.

We give evidence for this conjecture in two ways: one in terms of theorems about characteristic polynomials for random matrices which reveal completely analogous behavior; the other is by explicit numerical examples, both for integral moments as well as real and even complex moments. We also present a heuristic method via approximate functional equations which leads to the conjectures. Our conjectures agree with all the known theorems (and several number theoretical conjectures) about moments of families of L-functions.

Exponents of torsion cosets and Salem numbers

Chris Smyth

We show that there are Salem numbers of every trace. The nontrivial part of this result is for Salem numbers of negative trace. The proof has two main ingredients. The first is a novel construction, using pairs of polynomials whose zeros interlace on the unit circle, polynomials of specified negative trace having one factor a Salem polynomial, with any other factors being cyclotomic. The second is an upper bound for the exponent of a maximal torsion coset of an algebraic torus in a variety defined over the rationals. This second result, which may be of independent interest, enables us to refine our construction to avoid getting cyclotomic factors, and so produce Salem polynomials of any specified trace.

Principal moduli and class fields

Peter Stevenhagen
(joint work with David Cox (Amherst) and John McKay (Concordia))

We study the Galois theoretic properties of the values taken by $\Gamma_0(n)$-modular functions at elliptic points of order 2 for the Fricke group $\Gamma_0(n)^\dagger$ that lie outside $\Gamma_0(n)$. In the case of a principal modulus ('Hauptmodul') for $\Gamma_0(n)$ or $\Gamma_0(n)^\dagger$, we determine the class fields generated by these values.

Deterministic equation solving over finite fields

Christiaan van de Woestijne

Introduction and results

Many algorithmic problems over finite fields have up to now only found a probabilistic solution, if one wants algorithms of polynomial time complexity. In particular, finding zeros of polynomial equations in general finite fields is a problem for which no deterministic fast algorithm is known.

In this note, I want to propose a deterministic polynomial time equation solver for a special class of polynomial equations, namely *homogeneous diagonal forms* in many variables.

Theorem 1. *There exists an algorithm which does the following. Given a positive integer n, a finite field $\mathbb{F}$ and nonzero elements $a_0, \ldots, a_n$ in $\mathbb{F}$, it finds $x_0, \ldots, x_n$ in $\mathbb{F}$, not all zero, such that*

$$\sum_{i=0}^{n} a_i x_i^n = 0, \tag{1}$$

in time polynomial in $\log |\mathbb{F}|$ and in n.

Here I assume the finite field given by a generating equation over the prime field, together with the characteristic. Note that equations like (1) are always solvable by the Chevalley-Warning theorem.

We have found an algorithm satisfying the above properties running in time

$$\mathcal{O}((\log |\mathbb{F}|)^4 \log\log |\mathbb{F}|\ n^5)\ ,$$

whose building blocks are summarized below.

Building blocks

Let $\mathbb{F}$ be a finite field, and write $q = |\mathbb{F}|$.

First one remarks that we can easily reduce to the case that the exponent n divides $q-1$. (This is not needed in the following results, however.)

Next, we have the following lemma:

Lemma 1. *Let $a_0, \ldots, a_n$ be nonzero elements of $\mathbb{F}$, and let G be the subgroup of $\mathbb{F}^*$ generated by the a_i. Then there exist two among the a_i, say a_0 and a_1, such that their quotient a_0/a_1 has an nth root in the group G.*

Furthermore, we can adapt the Tonelli-Shanks algorithm for computing square (and higher) roots into a deterministic polynomial time algorithm to compute such an nth root. We will call this the n-Shanks algorithm[1].

Lemma 2. *Given a positive integer n, we can find deterministically, in polynomial time $x_0, \ldots, x_n$ in $\mathbb{F}$, not all zero, such that*

$$\sum_{i=0}^{n} x_i^n = 0. \tag{2}$$

There exists an algorithm for the task described in the lemma which uses among other things $\tilde{\mathcal{O}}(n)$ calls of the n-Shanks algorithm. Of course, the task is trivial if n (or just $\gcd(n, q-1)$) is odd. As an example for the even n, our algorithm can write -1 as a sum of squares deterministically in time $\mathcal{O}((\log q^4))$.

Lemma 3. *Given a solution to* (2) *and given $a_0, \ldots, a_n$, we can construct a solution to* (1) *deterministically, in polynomial time.*

Here the running time is essentially given by the cost of n^2 calls to the n-Shanks algorithm.

Applications

The algorithm described above is practical and has been implemented by the author. However, probabilistic methods for solving (1) usually run faster, except in the case that q is about as large as n^2, because here the Weil bound says nothing about the minimum number of solutions.

It may be interesting to note that the algorithm favours solutions with many zero components, although it is not clear whether the solutions it finds are always minimal in this respect.

(This work is part of my ongoing thesis project under supervision of Prof. H.W. Lenstra, Jr.)

Arithmetic of Calabi–Yau Varieties and Mirror Symmetry

Noriko Yui

1. Introduction

Definition 1.1. A smooth projective variety X of dimension d over $\mathbb{C}$ is a *Calabi–Yau* variety if

(1) $H^i(X, \mathcal{O}_X) = 0$ for every i, $0 < i < d$, and

(2) the canonical bundle of X is trivial.

Introduce the (i,j)-th Hodge number $h^{i,j}(X) := \dim H^j(X, \Omega_X^i)$. Then (1) simply says that $h^{i,0}(X) = 0$ for every i, $0 < i < d$ and (2) says that the geometric genus $p_g(X) := h^{d,0}(X) = 1$. There is the Hodge diamond encoding all Hodge numbers of a Calabi–Yau variety of dimension d.

[1]Suggestions for a better name are welcome!

Examples 1.1. For $d = 1$, the dimension one Calabi–Yau varieties are nothing but elliptic curves.

For $d = 2$, the dimension two Calabi–Yau varieties are K3 surfaces, where $h^{1,1}(X) = 20$. For $d = 3$, we have Calabi–Yau threefolds if $h^{1,1}(X) > 0$. The Euler characteristic of elliptic curves and K3 surfaces are given, respectively, by the fixed constants 0 and 24. However, this is no longer the case of Calabi–Yau threefolds. In fact, the Euler characteristic of a Calabi–Yau threefold X is given by $\chi(X) = 2(h^{1,1}(X) - h^{2,1}(X))$. There is a conjecture (by physicists) which asserts the existence of the absolute constant C such that $|\chi(X)| \leq C$. (The current record is $C = 960$.) However, there is also a counter-conjecture by M. Reid asserting the contrary.

A naive version of the mirror symmetry conjecture for Calabi–Yau threefolds can be formulated as follows.

Conjecture 1. Given a family of Calabi–Yau threefolds X, there is a mirror family of Calabi–Yau threefolds X^* such that

$$h^{1,1}(X^*) = h^{2,1}(X),\ h^{2,1}(X^*) = h^{1,1}(X)$$

(so that $\chi(X^*) = -\chi(X)$).

There are about $60,000,000$ examples of Calabi–Yau threefolds obtained by Batyrev's method (i.e., corresponding to reflexive polytopes). They were plotted by H. Skarke (Oxford).

Our Goal: *To understand the mirror symmetry phenomena by means of the zeta-functions and L-series of mirror pairs of Calabi–Yau threefolds.*

This will lead us to massive computations of the zeta-functions and L-series, and accordingly, it will fit in the main theme of this workshop.

2. The modularity questions of Calabi–Yau varieties over $\mathbb{Q}$

Let X be a Calabi–Yau variety of dimension d defined over $\mathbb{Q}$. Let

$$L(X, s) := L(H^d_{et}(X), s)$$

be the (cohomological) L-series of X. (Since L-series of algebraic varieties over $\mathbb{Q}$ were defined by an earlier talk in the workshop, I will not repeat the definition here.) The computation of the L-series $L(X, s)$ for a Calabi–Yau variety X over $\mathbb{Q}$ is the main topic here. For this we will address the modularity question.

$\boxed{d = 1}$: For $d = 1$, we have the celebrated theorem due to Wiles et al. Let E be an elliptic curve over $\mathbb{Q}$ with conductor N. Then the L-series $L(E, s)$ can be determined locally by counting the number of $\mathbb{F}_p$-rational points on $E \pmod p$ for good primes p. That is,

$$L(E, s) = \prod_p \frac{1}{1 - t_1(p)p^{-s} + \varepsilon(p)p^{1-2s}}$$

where the product runs over all primes p. If $p \not| N$, $t_1(p) = p + 1 - \#E(\mathbb{F}_p)$ (which is the trace of the Frobenius on $H^1_{et}(E, \mathbb{Q}_\ell)$) and $\varepsilon(p) = 1$; if $p \mid N$, $t_1(p) = 0$, or ± 1, and $\varepsilon(p) = 0$. The celebrated theorem of Wiles et al. asserts that there is a global object which determine the L-series $L(E, s)$.

Theorem 2.1. *Every elliptic curve E over $\mathbb{Q}$ is modular. That is, there is a cups form $f \in S_2(\Gamma_0(N))$ such that*

$$L(E, s) = L(f, s).$$

In Wiles' proof, the prime 3 played prominent roles, backed up by the prime 5.

$\boxed{d=2}$: Now we pass onto Calabi–Yau varieties of dimension 2, namely, K3 surfaces. The second Betti number of any K3 surface is equal to 22, and $H^2(X,\mathbb{Z})$ is a lattice of rank 22 isometric to $U_2^3 \oplus (-E_8)^2$. Let $NS(X)$ be the Néron–Severi group X parametrized by algebraic cycles on X. $NS(X)$ is a free finitely generated abelian group. Let $\rho(X)$ be its rank (called the Picard number of X). Since $NS(X) \subset H^2(X,\mathbb{Z}) \cap H^{1,1}(X,\mathbb{R})$, it follows that $\rho(X) \leq 20$. We let $T(X)$ be the orthogonal complement of $NS(X)$ in $H^2(X,\mathbb{Z})$ (with respect to the intersection pairing). We call it the group of transcendental cycles on X.

Now assume that X is defined over $\mathbb{Q}$. Let $L(X,s) = L(H^2_{\acute{e}t}(X),s)$ be the L-series of X. Then the L-series $L(X,s)$ factors (over $\mathbb{Q}_\ell$, and hence over $\mathbb{Q}$) as $L(NS(X),s)\cdot L(T(X),s)$. The Tate conjecture (which is a theorem for any K3 surface in characteristic 0) asserts that the order of zeros of the L-series at $s=2$ is equal to the Picard number $\rho(X)$.

We restrict to a special class of K3 surfaces.

Definition 2.1. A K3 surface X is called *extremal* (or *singular*) if $\rho(X) = 20$.

Note that if X is an extremal K3 surface over $\mathbb{Q}$, then $T(X)$ corresponds bijectively to a positive definite even binary quadratic form, and hence X is of CM type. The modularity of any extremal K3 surface over $\mathbb{Q}$ follows from a theorem of Livné.

Theorem 2.2. *Let X be an extremal K3 surface defined over $\mathbb{Q}$. Then the transcendental part of X is modular. That is, there is a cups form $f \in S_3(\Gamma_0(M),\varepsilon)$ for some $M \in \mathbb{N}$ and a quadratic character ε such that*

$$L(T(X),s) = L(f,s).$$

$\boxed{d=3}$: Now we consider Calabi–Yau threefolds.

Definition 2.2. A Calabi–Yau threefold X is called *rigid* if $h^{2,1}(X) = 0$ (so that $B_3(X) = 2$). If $h^{2,1}(X) \neq 0$, X is said to be *non-rigid*.

Remark 2.1. The Hodge number $h^{2,1}(X)$ is the dimension of the deformation space of X. So any rigid Calabi–Yau threefold has no deformation parameters. One implication of this is that rigid Calabi–Yau threefolds have no mirror partners which are Calabi–Yau threefolds. In other words, the mirror symmetry conjecture fails for rigid Calabi–Yau threefolds. However, physicists suggest that mirror partners of rigid Calabi–Yau threefolds might be Fano varieties in $\mathbb{P}^8$.

We now address the modularity of rigid Calabi–Yau threefolds over $\mathbb{Q}$. Let $L(x,s)$ be the L-series of a rigid Calabi–Yau threefold X over $\mathbb{Q}$. It is given by taking the product of the local zeta-function for every prime p:

$$L(X,s) = L(H^3_{et}(X,\mathbb{Q}_\ell),s) = (*) \prod_{p:\text{good}} \frac{1}{1 - t_3(p)p^{-s} + p^{3-2s}}$$

where $(*)$ corresponds to bad primes. Let $t_i(p)$ denote the trace of the Frobenius on $H^i_{et}(X,\mathbb{Q}_\ell)$. Then the Lefschetz fixed point formula gives $t_3(p) = 1 + p^3 + (1+p)t_2(p) - \#X(\mathbb{F}_p)$ with $t_2(p) \leq ph^{1,1}$ and the equality holds if all cycles in $H^{1,1}(X)$ are defined over $\mathbb{Q}$.

Conjecture 2. Let X be a rigid Calabi–Yau threefold defined over $\mathbb{Q}$. Then X is modular. That is, there is a cusp form $f \in S_4(\Gamma_0(N))$ such that

$$L(X,s) = L(f,s).$$

Here N is divisible only by bad primes.

Evidence: *Up to date, there are "about" 40 rigid Calabi–Yau threefolds over X for which the modularity is established.*

Some of these 40 rigid Calabi–Yau threefolds may be birationally equivalent over $\mathbb{Q}$. We have not yet checked the existence of such morphisms, and this is the reason for "about" in the statement.

Methods: There are several methods for proving the modularity of rigid Calabi–Yau threefolds:

(a) Serre–Faltings' criterion (to establish the equivalence between two 2–dimensional Galois representations).

(b) Geometric structure, that is, given a rigid Calabi–Yau threefold X over $\mathbb{Q}$, find a birational transformation (or a correspondence) defined over $\mathbb{Q}$ to a known rigid Calabi–Yau threefold.

(c) Wiles' method recently obtained by Dieulefait and Manoharmayum: *Suppose that X satisfies one of the following two conditions: (1) X has good reduction at 3 and 7, or (2) X has good reduction at 5 and some prime $p \equiv \pm 2 \pmod 5$ with $5 \not| t_3(p)$, then X is modular.*

There was no time to discuss non-rigid Calabi–Yau threefolds and their modularity, nor the computations of the zeta-functions and L-series of mirror pair families of Calabi–Yau threefolds.

If you are interested in arithmetic aspects of Calabi–Yau varieties and mirror symmetry, please take a look at a conference proceedings will be published in the Fields Communication Series Vol. 38 *Calabi–Yau Varieties and Mirror Symmetry* from the American Mathematical Society in October 2003. (ISBN 0-8218-3355-3).

Edited by Bill Allombert

Participants

Prof. Dr. Bill Allombert
allomber@math.u-bordeaux.fr
INRIA NANCY / LORIA
Boite Postale 239
F-54506 Vandoeuvre les Nancy Cedex

Dr. Roberto M. Avanzi
mocenigo@exp-math.uni-essen.de
Institut f. Experimentelle Mathem.
Universität Duisburg-Essen
Standort Essen
Ellernstr. 29
D–45326 Essen

Prof. Dr. Karim Belabas
Karim.Belabas@math.u-psud.fr
Mathematiques
Université Paris Sud (Paris XI)
Centre d'Orsay, Bâtiment 425
F-91405 Orsay Cedex

Prof. Dr. Daniel J. Bernstein
djb@cr.yp.to
Department of Mathematics
University of Illinois at Chicago
M/C 249, 322 SEO
851 S. Morgan Street
Chicago IL-60607-7045 – USA

Prof. Dr. Manjul Bhargava
bhargava@math.princeton.edu
Dept. of Mathematics
Harvard University
1 Oxford Street
Cambridge MA 02138-2901 – USA

Prof. Dr. Yuri Bilu
yuri@math.unibas.ch
Yuri.Bilu@math.u-bordeaux.fr
Mathématiques et Informatique
Université Bordeaux I
351, cours de la Libération
F-33405 Talence Cedex

Wieb Bosma
bosma@sci.kun.nl
Mathematisch Instituut
Katholieke Universiteit Nijmegen
Toernooiveld 1
NL-6525 ED Nijmegen

Dr. Dongho Byeon
dhbyeon@math.snu.ac.kr
School of Mathematical Sciences
Seoul National University
Seoul 151-747 – Korea

Prof. Dr. Frank Calegari
fcale@math.harvard.edu
Dept. of Mathematics
Harvard University
1 Oxford Street
Cambridge MA 02138-2901 – USA

Robert Carls
carls@math.leidenuniv.nl
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Henri Cohen
cohen@math.u-bordeaux.fr
Laboratoire A2X
UFR de Math. et Informatique
Université de Bordeaux I
351, cours de la Libération
F-33405 Talence Cedex

Prof. Dr. Jean-Marc Couveignes
couveig@univ-tlse2.fr
GRIMM, UFR SES
Université Toulouse II
5, Allée Antonio Machado
F-31058 Toulouse

Prof. Dr. John E. Cremona
John.Cremona@nottingham.ac.uk
Dept. of Mathematics
The University of Nottingham
University Park
GB-Nottingham, NG7 2RD

Prof. Dr. Tim Dokchitser
tim.dokchitser@durham.ac.uk
Dept. of Mathematical Sciences
The University of Durham
Science Laboratories
South Road
GB-Durham, DH1 3LE

Prof. Dr. Bas Edixhoven
edix@math.leidenuniv.nl
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Philippe Elbaz-Vincent
pev@math.univ-montp2.fr
Departement de Mathematiques
Université Montpellier II
Place Eugène Bataillon
F-34095 Montpellier Cedex 5

Prof. Dr. Noam D. Elkies
elkies@math.harvard.edu
Dept. of Mathematics
Harvard University
1 Oxford Street
Cambridge MA 02138-2901 – USA

Prof. Dr. Eugene Victor Flynn
evflynn@liv.ac.uk
Dept. of Pure Mathematics
The University of Liverpool
P. O. Box 147
GB-Liverpool L69 3BX

Eduardo Friedman
friedman@uchile.cl
Depto. Matematicas
Universidad de Chile
Casilla 653
Santiago – Chile

Dr. Herbert Gangl
herbert@mpim-bonn.mpg.de
Max-Planck-Institut für Mathematik
Vivatsgasse 7
D–53111 Bonn

Prof. Dr. Paul E. Gunnells
gunnells@math.umass.edu
Dept. of Mathematics & Statistics
University of Massachusetts
Amherst, MA 01003-9305 – USA

Dr. Jürgen Klüners
klueners@mathematik.uni-kassel.de
FB 17 - Mathematik/Informatik -
Universität Kassel
Heinrich-Plett-Str. 40
D–34132 Kassel

David R. Kohel
kohel@math.usyd.edu.au
School of Mathematics & Statistics
University of Sydney
Sydney NSW 2006 – Australia

Dr. Alan Lauder
alan.lauder@comlab.ox.ac.uk
St. John's College
Oxford University
GB-Oxford OX1 3JP

Dr. Franz Lemmermeyer
hb3@ix.urz.uni-heidelberg.de
Schlossgraben 7
D–73485 Unterschneidheim

Prof. Dr. Hendrik W. Lenstra, Jr.
hwl@math.berkeley.edu
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Ronald van Luijk
rmluijk@math.berkeley.edu
Department of Mathematics
University of California
at Berkeley
Berkeley, CA 94720-3840 – USA

Prof. Dr. Jean-Francois Mestre
mestre@math.jussieu.fr
U. F. R. de Mathematiques
Case 7012
Université de Paris VII
2, Place Jussieu
F-75251 Paris Cedex 05

Dr. Preda Mihailescu
preda@upb.de
FB 17: Mathematik - Informatik
D 344
Universität Paderborn
Warburger Str. 100
D–33098 Paderborn

Prof. Dr. Michael E. Pohst
pohst@math.tu-berlin.de
Fakultät II -Institut f. Mathematik
Technische Universität Berlin
Sekr. MA 8-1
Straße des 17. Juni 136
D–10623 Berlin

Prof. Dr. Carl Pomerance
carlp@math.uga.edu
Department of Mathematics and
Computer Science
Dartmouth College
6188 Bradley Hall
Hanover, NH 03755-3551 – USA

Prof. Dr. Bjorn Poonen
poonen@math.berkeley.edu
Department of Mathematics
University of California
at Berkeley
Berkeley, CA 94720-3840 – USA

Prof. Dr. Xavier Roblot
roblot@desargues.univ-lyon1.fr
Institut Girard Desargues
Université Claude Bernard
43, Bd. du 11 Novembre 1918
F-69622 Villeurbanne Cedex

Prof. Dr. Fernando Rodriguez Villegas
villegas@math.utexas.edu
Department of Mathematics
University of Texas at Austin
1 University Station C/200
Austin, TX 78712-1082 – USA

Prof. Dr. Mike Rubinstein
miker@math.utexas.edu
American Institute of Mathematics
360 Portage Ave.
Palo Alto, CA 94306 – USA

Prof. Dr. Rene Schoof
schoof@science.uva.nl
Dipartimento di Matematica
Universita di Roma 2
Tor Vergata
I-00133 Roma

Dr. Bart de Smit
desmit@math.leidenuniv.nl
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Dr. Chris J. Smyth
c.smyth@edinburgh.ac.uk
School of Mathematics
University of Edinburgh
James Clerk Maxwell Bldg.
King's Building, Mayfield Road
GB-Edinburgh, EH9 3JZ

Prof. Dr. Harold M. Stark
stark@math.ucsd.edu
stark@euclid.ucsd.edu
Dept. of Mathematics
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0112 – USA

Peter Stevenhagen
psh@math.leidenuniv.nl
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Dr. Michael Stoll
m.stoll@iu-bremen.de
School of Engineering and Science
International University Bremen
Postfach 750561
D–28725 Bremen

Ulrich Vollmer
uvollmer@cdc.informatik.tu-darmstadt.de
Technische Universität Darmstadt
Fachbereich Informatik
Alexanderstr. 10
D–64283 Darmstadt

Christiaan van de Woestijne
cvdwoest@math.leidenuniv.nl
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Noriko Yui
yui@mast.queensu.ca
Department of Mathematics and Statistics
Queen's University
Kingston, Ontario K7L 3N6 – Canada

Prof. Dr. Don B. Zagier
zagier@mpim-bonn.mpg.de
Max-Planck-Institut für Mathematik
Vivatsgasse 7
D–53111 Bonn