

COUNTING POINTS ON VARIETIES: ABSTRACTS

MANJUL BHARGAVA: GALOIS CLOSURE FOR RINGS

We all learn the notion of "Galois closure" or "normal closure" for a finite extension of fields. But what might we mean by the "Galois closure" of an extension of rings? (joint work with Matthew Satriano, based on conversations with Hendrik Lenstra, Jean-Pierre Serre, Bart de Smit, and Kiran Kedlaya)

ANTOINE CHAMBERT-LOIR: VOLUME ESTIMATES IN ANALYTIC OR ADELIC GEOMETRY

Recent work on Manin's conjecture concerning the number of points of bounded height in algebraic varieties and its asymptotic behaviour have shown the importance of a geometric analogue, namely the asymptotic behaviour of the volume of adelic subspaces defined by some kind of height inequalities. This behaviour has been mostly studied in the framework of algebraic groups. We explain how the analytic behaviour of analogues of Igusa zeta functions, together with Tauberian theorems, allow to recover these properties, proving them in a very general geometric situation. This is joint work with Yuri Tschinkel.

JEAN-MARC COUVEIGNES : USING TORSION POINTS

Many constructions in algorithmic number theory use (Galois action on) roots of unity. It is well known, for example, that roots of unity produce very efficient normal bases for some very specific finite fields extensions. In this talk, I will recall some of these classical constructions, then explain what one can gain from replacing roots of unity by torsion points of elliptic curves in this context.

TIM DOKCHITSER: PARITY CONJECTURE FOR ELLIPTIC CURVES

For an elliptic curve E over a number field K , there are various 'modulo 2' versions of the Birch-Swinnerton-Dyer Conjecture, each sometimes called the Parity Conjecture. One asserts that the algebraic rank of E/K has the same parity as the analytic rank, as given by the root number. Another one is the same statement for the p -Selmer rank for some prime p . I will explain the proof of the fact that the first conjecture is implied by finiteness of the Tate-Shafarevich group, and the proof of the second conjecture for all E/Q and all p (completing earlier work by Birch, Stephens, Greenberg, Guo, Monsky, Nekovar and Kim). This is joint work with Vladimir Dokchitser.

THOMAS GEISSER: ON SUSLIN'S SINGULAR HOMOLOGY

Suslin and Voevodsky proved that over an algebraically closed field with finite coefficients prime to the characteristic, Suslin's singular homology is dual to étale cohomology. I will discuss the situation at the characteristic, over non-algebraically closed fields, and a Weil-étale version of Suslin homology.

EVERETT HOWE AND PETER STEVENHAGEN: GENUS-2 CURVES AND
JACOBIANS WITH A GIVEN NUMBER OF POINTS

This is a report on joint work with Kristin Lauter. While the theme of the conference is the problem of counting points on varieties — that is, given a variety, compute its number of points — we look at a complementary problem: Given a non-negative integer n , construct a variety (of some given type) that has exactly n points. We show that for infinitely many values of n , any simple ordinary abelian surface A over any finite field \mathbf{F}_q such that $\#A(\mathbf{F}_q) = n$ must have CM by a quartic field of discriminant larger than $n^{1/2}$. This means that a natural CM algorithm for producing a genus-2 curve over some finite field whose Jacobian has n points takes time (in the worst case) exponential in $\log n$. On the other hand, for most values of n we can explicitly construct a genus-2 curve over some finite field that has exactly n points in time polynomial in $\log n$, under standard heuristic assumptions.

KIRAN KEDLAYA: COMPUTING ZETA FUNCTIONS OF HYPERELLIPTIC CURVES

Suppose we are given (via a defining equation) a hyperelliptic curve of genus g over a finite field \mathbf{F}_q . What is the best algorithm for determining its zeta function? In fact, as one varies the range of the parameters, a number of wildly different techniques appear; I'll survey a few of these.

STEPHEN LICHTENBAUM: FORMULAS FOR SPECIAL VALUES OF ZETA-FUNCTIONS

If X is a variety over a finite field, conjectural formulas for special values of its zeta-function have been given by Milne and Geisser in terms of Euler characteristics of certain cohomology groups. We will discuss these formulas and possible analogues for schemes over number rings.

BAPTISTE MORIN: ON THE WEIL-ÉTALE FUNDAMENTAL GROUP

We discuss the Weil-étale cohomology for number fields, recently introduced by Lichtenbaum, from the point of view of topos theory. We define a fundamental group and give some examples. Then we show that this group leads to the computation of the Weil-étale cohomology.

EMMANUEL PEYRE: FREEDOM AND GOODNESS

When considering the points of bounded height on varieties with a big anti-canonical line bundle, various accumulating subsets emerge naturally. This led to the quest for a criterion to separate good rational points from bad ones. The notion of very free rational point, which is directly inspired by the notion of very free rational curve, seems to be a good candidate for such a criterion. In this talk, we shall introduce this notion and describe its application to several examples.

CARL POMERANCE: SOCIABLE NUMBERS

Consider iterating the function which sends a natural number to the sum of its proper divisors. A fixed point for this system, such as 6 or 28, is called perfect, while a number belonging to a cycle of length 2, such as 220 or 284, is called amicable. Known to Euclid and Pythagoras, some scholars have even found allusions to perfect and amicable numbers in the Old Testament. Sociable numbers are the natural generalization of perfect and amicable numbers to cycles of arbitrary length - they

are mere youngsters, having been studied for only a century! This talk will describe the colorful history of the problem (with more connections to Hendrik Lenstra than you might imagine) and report on some recent results on the distribution of sociable numbers within the natural numbers.

C. S. RAJAN: SOME QUESTIONS ON THE SPECTRUM AND ARITHMETIC OF
LOCALLY SYMMETRIC SPACES

We consider the question that the spectrum and the arithmetic of locally symmetric spaces should mutually determine each other. We interpret this in an automorphic context.

NIRANJAN RAMACHANDRAN: REMARKS ON CREW-MILNE FORMULA

An old formula of Crew and Milne (independently) relates the de Rham-Witt numbers and the Hodge numbers of a smooth projective variety over a perfect field of positive characteristic. The talk will indicate the proof of a generalized formula and sketch applications to the special values of zeta functions of motives over finite fields.

SAMIR SIKSEK: EXPLICIT CHABAUTY OVER NUMBER FIELDS

Let C be a curve of genus at least 2 over a number field K of degree d . Let J be the Jacobian of C and r the rank of the Mordell-Weil group $J(K)$. Chabauty is a practical method for explicitly computing $C(K)$ provided $r \leq g - 1$. In unpublished work, Wetherell suggested that Chabauty's method should still be applicable provided the weaker bound $r \leq d(g - 1)$ is satisfied. We give details of this and use it to solve the Diophantine equation $x^2 + y^3 = z^{10}$ by reducing the problem to determining the K -rational points on several genus 2 curves over $K = \mathbf{Q}(\sqrt[3]{2})$.

TONY VÁRILLY-ALVARADO: COX RINGS OF BIG RATIONAL SURFACES

Cox rings of del Pezzo surfaces have been used by several authors to count points of bounded height and thus verify instances of Manin's conjecture on the subject. We will show that the more general class of smooth projective rational surfaces with big anticanonical class has a finitely generated Cox ring. We will also present some systematic collections of examples of these surfaces. This is joint work with D. Testa and M. Velasco.

DAQING WAN: COUNTING POINTS WITH DISTINCT COORDINATES

I will give an expository talk on counting the number of rational points with distinct coordinates on certain higher dimensional affine symmetric varieties defined over a finite field, as well as its applications in graph theory, coding theory and computer sciences. (Joint work with Qi Cheng and with Jiyou Li).

OLIVIER WITTENBERG: EXISTENCE OF ZERO-CYCLES ON FIBRATIONS OVER
NUMBER FIELDS

For arbitrary smooth and proper varieties over a number field, Kato, Saito and Colliot-Thélène proposed around 1990 precise conjectures on the existence of zero-cycles satisfying local conditions. Thanks to work of Saito, Salberger, Colliot-Thélène and Frossard, these conjectures are now known for fibrations, over curves

with finite Tate-Shafarevich group, into Severi-Brauer varieties with squarefree index. In this talk I will present extensions of these results to more general fibrations.