Abstracts.

Abrashkin, Victor
"*Local analogue of the Grothendieck Conjecture*".

Let K_1 and K_2 be 1–dimensional complete discrete valuation fields with the same separable closure L. For $i = 1, 2$, set $\Gamma_{K_i} = \mathrm{Gal}(L/K_i)$ and consider its decreasing filtration via higher ramification subgroups $\{\Gamma_{K_i}^{(v)}\}_{v\geqslant 0}$. The local analogue of the Grothendieck Conjecture states that any topological group isomorphism $\alpha : \Gamma_{K_1} \longrightarrow \Gamma_{K_2}$ such that $\alpha(\Gamma_{K_1}^{(v)}) = \Gamma_{K_2}^{(v)}$ for all $v \geqslant 0$, comes from some continuous automorphism of the field L (which induces a field isomorphism of K_1 and K_2).

This statement was first proved in the case of local fields of characteristic 0 by Sh. Mochizuki (Intern. J. Math., v.8, no.4, 1997, 499–506) by an elegant application of Hodge–Tate theory. Using a more direct approach based on an explicit description of ramification filtration for local fields of finite characteristic (cf. Izvestiya RAN, v.62, no.5, 1998) the author considered the case of local fields of arbitrary characteristic with residue fields of characteristic > 2 (Preprint IML, Luminy, 22, 1998). Recently this approach was generalized to the case of n–dimensional local fields of finite characteristic (the higher ramification theory of such fields was developped by I.Zhukov, cf. Preprint 98–03, University of Nottingham, for the case $n = 2$).

Acciaro, Vincenzo & Fieker, Claus
"*Finding normal integral bases of cyclic number fields of prime degree*".

Let $L = \mathbb{Q}[\alpha]$ be a cyclic number field of prime degree p, and let us assume that an integral basis for L is known. We describe a new algorithm which decides if L possesses a normal integral basis and, in the affirmative case, computes it efficiently. A well known criterion to compute a normal integral basis of a cyclic number field of prime degree yields an algorithm whose complexity depends on the size of the conductor $\mathfrak{f}$ of the field – instead, the complexity of our algorithm is independent on

the size of $\mathfrak{f}$. We reduce our problem to the problem of finding the generator of a principal ideal in the p–th cyclotomic field.

Aliev, Iskander
"*Weyl Sequences: Asymptotic Distributions of the Partition Lengths*".

Let θ be an irrational number in $[0, 1)$ and $x_k = k\theta \pmod 1$ for $k = 1, 2, \ldots$. The collection of points $W_n(\theta) = \{x_1, \ldots, x_n\}$ is sometimes called the Weyl sequence of order n.

In the present work we derive asymptotic distributions of different characteristics associated with the interval lengths of the partitions of $[0, 1)$ generated by $W_n(\theta)$. The main result establishes the two–dimensional asymptotic distribution of

$$(n \min\{x_1, \ldots, x_n\},\, n(1 - \max\{x_1, \ldots, x_n\}))$$

when $n \to \infty$. It then yields a number of results concerning the asymptotic distributions of one–dimensional characteristics.

There is a close relationship between the Weyl and Farey sequences. The present work thus also studies some distributional properties of the Farey sequences.

Andreatta, Fabrizio
"*On Mumford's uniformization of Jacobians*".

The construction of the Tate curve has been vastly generalized to higher dimensional semiabelian schemes by Mumford, Faltings and Chai allowing the construction of compactifications of the moduli space of principally polarized abelian varieties and establishing an algebraic theory of the q expansion of modular forms. Very little is known about this construction for the Pic^0 of semistable curves. We try to describe it for some special classes of curves using deformation theory.

Antoniadis, Jannis A.
"*Groups of Automorphisms of Algebraic Curves*".

We are going to describe some results concerning the group of automorphisms of some classes of algebraic curves such as of Fermat type, of the form

$$y^n = f(x)$$

of modular curves $X(N)$ and Fermat hypersurfaces. The results are contained in the Ph.D. Thesis of my student Dr. Aristides I. Kontogeorgis

Bayer–Fluckiger, Eva
"*Lattices and number fields*".

One of the oldest results of algebraic number theory is Gauss' correspondence between ideals of quadratic fields and binary quadratic forms. If K is a number field of any degree and O an order of K, one can define lattices on O–ideals in a way that extends Gauss' construction. These will be called *O–lattices*. If the degree of K is greater than 2, one does not obtain a bijective correspondence this way. It is natural to ask which lattices arise from a given order, and, for a given lattice, which orders give rise to it. On the other hand, O–lattices occur in several mathematical subjects as well as in information theory. The problems arising in these applications can be formulated in terms of the above questions, as well as in terms of certain (Arakelov) class groups.

Berhuy, Grigory
"*Caractérisation de formes trace hermitiennes sur des algèbres étales*".

Soit E une algèbre étale de rang fini sur k, c'est–à–dire un produit fini d'extensions finies séparables de k. On a alors une trace $\mathrm{Tr}_{E/k}$. A tout élément $\lambda \in E^*$, on associe une forme quadratique non dégénérée, appelée *forme trace amplifiée*, définie par $x \mapsto \mathrm{Tr}_{E/k}(\lambda x^2)$. Lorsque $\lambda = 1$, la forme quadratique obtenue est appelée *forme trace de E/k*. Si (E,λ) et (F,μ) sont deux algèbres étales de rang fini sur k, avec des éléments inversibles distingués, on dit qu'elles sont isomorphes s'il existe un k–isomorphisme de E sur F qui envoie λ sur μ. La forme trace amplifiée définie plus haut est alors un invariant de la classe d'isomorphisme de (E,λ).

Ce sont les formes trace qui ont été le plus souvent étudiées de manière systématique. Sans hypothèse sur k, on ne sait pas dire grand chose sur cette forme trace. Soit n est le rang de E/k. Si $n = 2^{m_1} + \cdots + 2^{m_h}, 0 \leq m_1 < \cdots < m_h$, alors Serre a montré que $\mathrm{Tr}_{E/k}(\langle 1 \rangle)$ contient la forme $\langle 2^{m_1}, \cdots, 2^{m_h} \rangle$. Si E est un corps, Serre a montré que l'invariant de Hasse–Witt de la forme trace d'une extension de corps mesurait l'obstruction à un certain problème de plongement galoisien. Si k est un corps hilbertien de caractéristique 0, alors Epkenhans et Kruskemper ont montré que la forme trace d'une algèbre étale de rang fini sur k était isomorphe à la forme trace d'une extension finie de k. Epkenhans a également montré que toute forme quadratique positive sur un corps de nombres (c'est–à–dire dont toutes les signatures sont positives) était isomorphe à la forme trace d'une extension finie de k. Ce n'est plus vrai si on suppose seulement que k est hilbertien.

Supposons maintenant que l'algèbre étale de rang fini E/k possède une involution k–linéaire σ. Alors on peut définir pour tout $\lambda \in E, \lambda^\sigma = \lambda$ une forme quadratique appelée *forme trace hermitienne amplifiée* par $x \mapsto \mathrm{Tr}_{E/k}(\lambda x x^\sigma)$. Si (E,σ,λ) et $F,\tau,\mu)$ sont deux algèbres étales de rang fini, munies d'involutions k–linéaires et d'éléments distingués symétriques, on dit qu'elles sont isomorphes s'il existe un isomorphisme

Φ de E sur F, qui envoie λ sur μ et tel que $\Phi(x^\sigma) = \Phi(x)^\tau$ pour tout $x \in E$. La forme trace hermitienne amplifiée précédente est alors un invariant de la classe d'isomorphisme de (E, σ, λ).

Il est naturel de se demander si on a l'analogue des théorèmes précédents dans ce cas. Le but de cet exposé est précisement de répondre à cette question. En fait, tout se passe le mieux possible. En effet, toute forme quadratique non dégénérée de dimension paire sur un corps hilbertien, et non isomorphe au plan hyperbolique, est isomorphe à une forme trace hermitienne amplifiée d'une extension finie séparable de k. En modifiant légèrement la démonstration, on montre que tout réseau sur l'anneau des entiers d'un corps de nombres de dimension paire, distinct du plan hyperbolique, peut s'obtenir à partir de formes trace hermitiennes amplifiées, et on donne une manière explicite de les calculer. Enfin, toute forme quadratique positive, de dimension paire sur un corps de nombres k, non dégénérée et non isomorphe au plan hyperbolique, est isomorphe à une forme trace d'une extension finie de k.

Bertolini, Massimo
"*p–adic L–functions and the arithmetic of elliptic curves*".

I will describe some recent results (in collaboration with Henri Darmon) on the relationship between the arithmetic of modular elliptic curves and the properties of certain anticyclotomic p–adic L–functions. These results are based on the theory of p–adic uniformization of Shimura curves and the theory of congruences between modular forms, combined with the features of the Euler System of Heegner points.

Bhowmik, Gautami
"*Zeta Functions of Subgroups of Abelian Groups*".

We establish a zeta function associated to the subgroups of finite abelian groups and prove that it is rational. The zeta function can be used to obtain good average orders of number of subgroups.

Bosma, Wieb
"*Signed bits and fast exponentiation*".

It is well-known that the binary method for computing powers (by repeated squaring and multiplication) is not always the fastest method. Depending on the exponent, there may exist addition chains the use of which requires fewer multiplications than the binary method; however, shortest addition chains are in general hard to determine. If the exponentiation takes place in a group in which inverses can be found efficiently, it is also possible to use a redundant representation of positive integers for exponentiation. Namely, if we write $e = \sum_{i=1}^{n} s_i 2^i$, where $s_i \in \{-1, 0, 1\}$, we have obtained a *signed bit* representation of e that can be used to compute x^e just like the ordinary bit representation (with $s_i \in \{0, 1\}$). The advantage of the signed bit representation is that it is not unique, and that among the various representations of e it may be possible to find one with smaller *weight* (fewer non-zero s_i) than the binary expansion.

Among the groups in which inverses can be found efficiently are the groups of points on elliptic curves in Weierstrass form over a field: finding the inverse of a point merely amounts to negating one of the coefficients, and is therefore an almost 'free' operation. These groups are of importance in many cryptographic applications.

It is also fairly well-known that there exists a particular signed bit representation that is unique and of minimal weight for any e, the *non-adjacent form*. In this talk we will derive the known facts about non-adjacent forms in an elementary way, and then proceed to give an exact, elementary analysis of the benefits of using the non-adjacent form for exponentiation. (The exact gain in using non-adjacent forms over the binary expansion depends on the relative costs of multiplication, inversion and squaring in the group; we treat some special cases.) To achieve this we simply count the number of non-adjacent forms of given length as well as their total weight. It turns out that this can be easily done using a simple recursion, leading to so-called Jacobsthal numbers. This way we derive an exact version of the heuristic result that on average only one in three signed bits is non-zero in the non-adjacent form (as opposed to one in two ordinary bits in the binary expansion).

Bouw, Irene I.
"*Reductions of covers and Hurwitz spaces*".

In this talk, we will study the compactified Hurwitz space classifying G-Galois covers of $\mathbb{P}^1$ in mixed characteristic p as introduced in a recent preprint of Abramovich–Oort. We will be interested in the case that p exactly divides the order of G, but does not divide the order of the ramification indices. Using results of Raynaud, one gets information on the possible reductions of G-covers of $\mathbb{P}^1$. This enables us to compute the irreducible components of the special fiber of the Hurwitz space, in certain cases. For instance, if $G = PSL_2(\ell)$, for some sufficiently small prime ℓ different from p, we get a complete description of the irreducible components and there intersection behavior. Joint work with Stefan Wewers.

Brisebarre, Nicolas
"*A recursive approach for solving some systems of difference equations*".

Let f a function solution of the system

$$\begin{cases} \displaystyle\sum_{0\le m\le M} P_m(z)f(z+m\alpha)=0, \\ \displaystyle\sum_{0\le n\le N} Q_n(z)f(z+n\beta)=0, \end{cases} \tag{1}$$

where $(P_m)_{0\le m\le M}$ and $(Q_n)_{0\le n\le N}$ are finite sequences of $\mathbb{C}[z]$ with $P_M Q_N \neq 0$, α et β being some complex numbers linearly independent on $\mathbb{Q}$. The study of such systems was, in particular, a consequence of a question of D. Masser [9]. J.-P. Bézivin and F. Gramain showed in [2] and [3] that it was possible to reduce the study to the case when the coefficients of the system are constant (the solution of this new system is no more the function f but the product of f by a polynomial). Hence, we can assume that our system has constant coefficients and we develop then a recursive method that allows to determine the continuous functions from $\mathbb{R}$ to $\mathbb{C}$, entire, or meromorphic solutions of the system. More precisely, we show that if f is continuous from $\mathbb{R}$ to $\mathbb{C}$ or entire and satisfies to (1) , it has necessarily the shape $\sum_{k=1}^{K} R_k(z)e^{\delta_k z}$ with R_k in $\mathbb{C}(z)$ and δ_k in $\mathbb{C}$ for every k (doing so, we find again the results of [1], [2], [3], [6] and [8]). If we assume that f is meromorphic, we prove that f is a linear combination, over the field of elliptic functions of periods α and β, of products of rational fractions by some functions constructed from Weierstrass σ and ζ functions. The latter case is also considered in [7] in which a more general result is obtained.

References:

[1] J.-P. Bézivin, *Sur les systèmes d'équations aux différences*, preprint.

[2] J.-P. Bézivin et F. Gramain, *Solutions entières d'un système d'équations aux différences*, Ann. Inst. Fourier **43**-3 (1993), 791–814.

[3] J.-P. Bézivin et F. Gramain, *Solutions entières d'un système d'équations aux différences II*, Ann. Inst. Fourier **46**-2 (1996), 465–491.

[4] N. Brisebarre, *An algorithm for finding integer solutions of systems of difference equations*, preprint.

[5] N. Brisebarre, *Une approche récursive pour la résolution de certains systèmes d'équations aux différences*, preprint.

[6] N. Brisebarre et L. Habsieger, *Sur les fonctions entières à double pas récurrent*, to appear in Annales de l'Institut Fourier.

[7] J.-C. Jolly et J.-J. Loeb, *Solutions méromorphes sur $\mathbb{C}$ d'un système de deux équations aux différences à coefficients constants*, preprint.

[8] J.-J. Loeb, *Sur certaines équations aux différences associées à des groupes*, preprint.

[9] D. Masser, *On certain functional equations in several variables*; Approximations diophantiennes et nombres transcendants, Luminy 1982, D. Bertrand et M. Waldschmidt eds, Progress in Math. **31**, 1983, 173–190. Birkhäuser, Boston.

Brüdern, Jörg
"*Artin's conjecture revisited: pairs of forms*".

This talk describes recent joint work with H. Godinho on Artin's conjecture for diagonal forms. It is shown that a pair

$$\sum_{j=1}^{s} a_j x_j^k = \sum_{j=1}^{s} b_j x_j^k = 0$$

with integer coefficients has solutions in all p-adic fields provided only that $s > 2k^2$ (as predicted by the conjecture), with one exception: when $k = p^t(p-1)$ with $t > 0$ we need $s > 4k^2$. The methods are largely combinatorial, with a new concept of colorings on the set of variables, and applications of combinatorial group theory.

Bruin, Nils
"*Solving generalized Fermat–Equations.*"

In 1994, H. Darmon and A. Granville proved that the equation $x^r + y^s = z^t$ with fixed $r, s, t \in \mathbb{Z}_{>0}$ and $1/r + 1/s + 1/t < 1$ has only finitely many solutions $x, y, z \in \mathbb{Z}$ with $\gcd(x, y, z) = 1$. An example like $43^8 + 96222^3 = 30042907^2$ shows that these equations sometimes do have some highly non–trivial solutions.

Such solutions turn out to correspond to rational points on finitely many algebraic curves of genus > 1. In this talk I will show how, in some cases, one can determine these curves explicitly and how to find the rational points on them.

The method used is based on the proof of a special case of Faltings' Theorem by C. Chabauty in 1941. It enabled me to solve the equation for $\{r, s, t\} = \{2, 4, 6\}$, $\{2, 3, 8\}$ and $\{2, 4, 5\}$. Additionally, the method is applicable to curves of genus 2 independent of the rank of the jacobian of the curve over $\mathbb{Q}$ (a Chabauty–style argument if the rank of the jacobian ≤ 1 was already described by R. F. Coleman and V. Flynn)

Bugeaud, Yann
"*On the Diophantine equation* $\frac{x^n-1}{x-1} = y^q$".

We present a survey of very recent results concerning the Diophantine equation

$$\frac{x^n - 1}{x - 1} = y^q, \qquad (*)$$

in integers $x > 1$, $n > 2$, $y > 1$ and $q > 1$, which has been extensively studied by (among others) Nagell, Ljunggren and Shorey. These new statements have been proved by Bennett, Bugeaud, Hanrot, Mignotte, Roy, Saradha, Shorey, and they include the following ones :

– (*) has no solution (x, y, n, q) with x being a square;

– (*) has no solution (x, y, n, q) with n congruent to 1 modulo q, except $(3, 11, 5, 2)$;

– If (*) has a solution $(x, y, n, q) \neq (18, 7, 3, 3)$, then there exists a prime p such that p divides x and q divides $p - 1$;

– (*) has only three solutions (x, y, n, q) with $x \leq 10^4$, namely $(3, 11, 5, 2)$, $(7, 20, 4, 2)$ and $(18, 7, 3, 3)$;
– The only solution (x, y, n, q) of (*) with $5 \mid n$ is $(3, 11, 5, 2)$.

In particular, jointly with Mignotte, we have proved that an integer > 1 with all digits equal to 1 in base ten cannot be a pure power. The proofs involve various techniques in diophantine approximation and in elementary number theory.

Bundschuh, Peter
"*Irrationality results by analytic methods*".

For fixed complex q with $|q| > 1$ let $F_q(x, y)$ denote the entire function $\Pi_{j \geq 0}(1 + q^{-j}x + q^{-2j}xy)$ of two complex variables x, y. Quite recently, D.S. Lubinsky and P. Zhou proved some irrationality results concerning the function F_q at points (x, y) with positive rational numbers x, y and for positive integers $q > 1$.

Using simpler arguments we extend their results by showing, that, under very natural hypotheses, $F_q(x, y)$ and $F_q(-x, -y)$ cannot both belong to K for non-zero x, y and integers q from K, where K denotes either the rational or an imaginary quadratic number field. We further strengthen these qualitative results by statements on the simultaneous approximation of $F_q(x, y)$ and $F_q(-x, -y)$ by numbers from K.

Some other applications of our method of proof shall be indicated.

Buzzard, Kevin
"*Families of modular forms*".

In many first courses on modular forms, the first explicit examples of non–zero forms are usually the Eisenstein series of level 1. These Eisenstein series visibly lie in a "family"—as the weight varies, the coefficients of the forms vary in a nice analytic way. Over the last 20 years, starting with work of Hida, and more recently of Gouvea–Mazur and of Coleman, it has become clear that in fact many modular forms live in families, in a very precise sense. I will explain something about what we know, what we don't know, and also why the problem of constructing families of modular forms is a worthwhile one.

Cai, Tianxin
"*Chains of primes or composites on* $f(x, y)$".

A chain is defined as a sequence of lattice points $\{(x_i, y_i) \mid 1 \leq i \leq n\}$ with $x_1 = y_n = 1, \mid x_i - x_{i+1} \mid + \mid y_i - y_{i+1} \mid \geq 1$ for $1 \leq i < n$. Let $f(x, y)$ be a binary arithmetic function. A chain of primes (composites) means a chain $\{(x_i, y_i)\}$ that $f(x_i, y_i)$ is always prime (composites).In this paper, we study for $f(x, y) = (ax + by)/(ax, by)$, we show that if a, b are positive integers, $(a, b) = 1, 2 \leq a + b \leq 5$, and the k–tuple prime conjecture is true, then there are infinitely many disjoint chains of primes on $f(x, y)$. Meanwhile, we prove other results and raise several questions concerning this topic, including one related with Goldbach conjecture.

Chambert-Loir, Antoine & Tschinkel, Yuri
"*The number points of bounded height in equivariant compactifications of affine spaces*".

Cohen, Henri
"*On the density of discriminants of number fields*".

(joint work with F. Diaz y Diaz and M. Olivier)

We show how the use of Kummer theory (as opposed to class field theory) allows to give explicit answers to questions such as the computation of the asymptotic density of extensions of a given base field for a given

Galois group G. We give explicit answers (for any base field) for $G = C_l$, (l prime or $l = 4$), $G = C_2 \times C_2$, $G = D_4$ (dihedral group with 8 elements) and we explain how our method can be used to find the density of A_4, and S_4 extensions, as well as D_l extensions for l prime.

Cohen, Paula
"*Applications de la Conjecture d'André–Oort à la transcendance*".

Dans cet exposé nous parlerons d'un travail en cours avec G. Wüstholz. Depuis 10 ans, la Conjecture d'André–Oort resiste à une solution sauf dans quelques cas particuliers résolus par Moonen et par André. Cette conjecture dit que, pour une sous-variété algébrique irréductible de l'espace modulaire de Siegel A_g de degré $g \geq 1$, la densité des points spéciaux sur cette sous-variété dans la topologie de Zariski entraine que la sous-variété est de type Hodge. D'après des travaux de moi-même, Shiga et Wolfart, on peut aussi détecter les points spéciaux dans A_g par un critère qui généralise celui de Schneider pour la fonction modulaire elliptique et qui provient de la théorie des nombres transcendants. Comme exemple particulier, nous montrerons comment la Conjecture d'André–Oort entraine des résultats sur la transcendance des valeurs spéciales des fonctions hypergéométriques.

Coleman, Mark D.
"*Averages of Arithmetic functions in number fields*".

A method due to Hooley and Huxley, presented in Acta Arith. **31** (9176) 313-324, gives results for averages over short intervals of arithmetic functions whose associated Dirichlet series have a given form. In this talk we present a generalization of this method to number fields. As an application of this generalization we might mention

Theorem. *For $m \geq 2, h \geq 1$ and all $z \in \mathbb{C}, |z| > 1$ we have that*

$$\sharp \{\alpha \in \mathbb{Z}[i] : |\alpha - z| \leq r(z), \omega(\alpha) = m, \Omega(\alpha) = m + h\}$$

has an asymptotic expansion of the form

$$\frac{(2\ell)^{n_K} x}{\log x} \sum_{0 \leq j \leq J(x)} \frac{P_{j,\mathbf{k}}(\log\log x)}{(\log x)^j} + O\left(x \ell^{n_K} \exp(-R(x))\right)$$

for some polynomials $P_{j,\mathbf{k}}(X)$, with $R(x) = \kappa_1 (\log x)^{1/3} (\log\log x)^{-1/3}$ and $J(x) = \kappa_2 (\log x)^{1/3} (\log\log x)^{-4/3}$. The result is valid for $|z| \exp(-R(|z|)) > r(z) > |z|^{7/12+\varepsilon}$, and the main term is

$$\frac{4r^2}{(m-2)!} \frac{(\log\log|z|)^{m-2}}{\log|z|} \sum_{\pi}{}' (N\pi)^{-(h+1)},$$

the sum being over unassociated primes of $\mathbb{Q}(i)$.

Cook, Roger J.
"*The values of additive forms at prime arguments.*

Montgomery and Vaughan have shown that the exceptional set in Goldbach's problem

$$E(X) = \#\{n \leq X : 2n \neq p_1 + p_2\}$$

satisfies

$$E(X) \ll X^{1-\Delta}$$

for some $\Delta > 0$.

Recently Brüdern, Cook and Perelli obtained an analogous result for binary linear forms with irrational coefficients. Instead of counting exceptional integers, suitably spaced real sequences mimic the role played by even integers in Goldbach's problem. An increasing sequence $v_1 < v_2 < \cdots$ of positive real numbers is called *well–spaced* if there exist positive constants $C > c > 0$ such that

$$0 < c < v_{i+1} - v_i < C \text{ for } i = 1, 2, \ldots .$$

The purpose of this paper is to prove the following analogous result.

Theorem. *Let $k \geq 2$ be an integer and $s = 2^{k-1} + 1$. Let $\lambda_1, \lambda_2, \ldots, \lambda_s$ be positive real numbers. Suppose that λ_1/λ_2 is irrational and algebraic. Let $\mathcal{V}$ be a well–spaced sequence. Let $\delta > 0$. Then the number $E_2(X)$ of $v \in \mathcal{V}$ with $v \leq X$ for which*

$$\left|\lambda_1 p_1^k + \lambda_2 p_2^k + \ldots + \lambda_s p_s^k - v\right| < v^{-\delta}$$

has no solution in primes $p_1, p_2, \ldots, p_s$ satisfies

$$E_2(X) \ll X^{1-\frac{1}{3\gamma}+2\delta+\epsilon}$$

for any $\epsilon > 0$, with $\gamma = 4^{k-1}$.

Coppola, Giovanni

"*On the distribution in the arithmetic progressions of reducible quadratic polynomials in short intervals,* I — II".

We study the distribution in the arithmetic progressions (modulo a product of two primes) of reducible quadratic polynomials $(an + b)(cn + d)$ in short intervals $[x, x + x^{\vartheta}]$, where $0 < \vartheta \leq 1$ (we include the case $\vartheta = 1$ of "long" intervals). In order to study the distribution of $n(n + 2)$ (the case of reducible quadratic polynomials $(an + b)(cn + d)$ gives the same results) in arithmetic progressions modulo a product of two primes (in the short interval $[x, x + h]$) we introduce the bilinear form over prime moduli, i.e.

$$\sum_{q\sim Q}\sum_{r\sim R}\gamma_q\delta_r \sum_{\substack{cx<n\leq x+h\\ n(n+2)\equiv 0(qr)}} 1,$$

where q and r are distinct primes and we assume that $QR > 2h + 2$.

We point out that the restriction to prime moduli is essential to our methods. We expect that

$$\sum_{q\sim Q}\sum_{r\sim R}\gamma_q\delta_r \sum_{\substack{cx<n\leq x+h\\ n(n+2)\equiv 0(qr)}} 1 = \sum_{q\sim Q}\sum_{r\sim R}\gamma_q\delta_r\left(\frac{2h}{qr} + \sum_{\substack{cx<n\leq x+h\\ n\equiv 0(qr)}} 1 + \sum_{\substack{cx<n\leq x+h\\ n\equiv -2(qr)}} 1\right) + O(h^{1-\varepsilon}), \tag{1}$$

when γ_q and δ_r are bounded arithmetical functions (as in the sequel) with support on the primes in the intervals $]Q, 2Q]$, $]R, 2R]$, respectively; here $(q, r) = 1$ and $1 \leq Q, R < h/2$.

In general, if the estimate over the odd square–free moduli d

$$\sum_{\substack{cx<n\leq x+h\\ n(n+2)\equiv 0(mod\, d)}} 1 = \frac{h}{d}\sum_{\substack{ct|d\\ \frac{d}{x+h}<t<x+h}} 1 + R_d(x, h)$$

holds on average over $d \sim D$, i.e. over $D < d \leq 2D$, with $D = x^{\alpha-\varepsilon}$ $(\forall\varepsilon \in]0, \alpha[)$ we say that the **distribution level** of the sequence (here $n(n + 2)$), in the arithmetic progressions, is (at least) α, provided $R_d(x, h)$ is, on average over d, a "good" error term (here $h = x^{\vartheta}$ is the length of the short interval).

For example, it can be shown by standard arguments that the distribution level of $n(n+2)$ is $\lambda \geq \vartheta$.

An important example of non–trivial treatment of the bilinear form of the error we quote is

$$\sum_{q\sim Q}\sum_{r\sim R}\gamma_q\delta_r \sum_{\substack{cn\leq x \\ n^2+1\equiv 0(qr)}} 1.$$

Iwaniec [3] in 1978 showed that the level of distribution in this case is $16/15$. Using this, he was able to prove that $n^2+1 = P_2$ for infinitely many n (here P_k denotes an integer with at most k prime factors), whilst the trivial level of distribution, that is 1, enables us to obtain only P_3.

Using the Large Sieve, we prove (see [1])

Theorem 1 *Let $x > 4,\ 3/4 < \vartheta \leq 1,\ x^\vartheta \leq h \leq x,\ 0 < \varepsilon < \frac{4\vartheta-3}{10}$. Then (1) holds, provided $R \leq h^2/x^{1+3\varepsilon},\ Q \leq h/x^{1/2+2\varepsilon}, QR > 2h+2$.*

Under the same hypotheses we get

Corollary 1 *The estimate (1) holds for $QR = x^{3\vartheta-3/2-5\varepsilon}$.*

Using the Dispersion Method we prove (see [2])

Theorem 2 *Let $x > 4,\ 0 < \vartheta \leq 1,\ x^\vartheta \leq h \leq x,\ 0 < \varepsilon \leq \frac{\vartheta}{4\vartheta+1}$. Then (1) holds provided $R \leq h^{1-2\varepsilon}, h^{2\varepsilon} \leq Q \leq R^{1/2}h^{-\varepsilon}, QR > 2h+2$.*

Under the same hypotheses we get

Corollary 2 *The estimate (1) holds for $QR = h^{3/2-4\varepsilon}$.*

Both theorems, whose methods are different in structure, improve on previous results of Salerno and Vitolo [4] based on Weil's estimate for Kloosterman sums.

References:

[1] Coppola, G. and Salerno, S., *On the distribution in the Arithmetic Progressions of Reducible Quadratic Polynomials in Short Intervals*, to appear.

[2] Coppola, G. and Salerno, S., *On the distribution in the Arithmetic Progressions of Reducible Quadratic Polynomials in Short Intervals ,II*, to appear.

[3] Iwaniec, H., *Almost–primes Represented by Quadratic Polynomials*, Inventiones Math. **47**, (1978) 171–188.

[4] Salerno, S. and Vitolo, A., *On the distribution in the arithmetic progressions of reducible quadratic polynomials*, Izwestiya Rossiyskoy AN, Math.Series **58** n.4, (1994) 211–223.

Cornelissen, Gunther
"*Class numbers, Eisenstein series and supersingular Drinfeld modules*".

When does the Jacobian of a hyperelliptic curve over a finite field $\mathbb{F}_q$ possess an $\mathbb{F}_q$–rational 2– or 4–torsion point? What is the distribution of the zeros of certain rigid analytic Eisenstein series for $GL(2)$? And what is the maximal number of supersingular primes of a given degree for a given rank–2 Drinfeld module? It is our aim to present some answers to these questions which highlight their (not so apparent) interrelation.

References:

[1] *Deligne's congruence and supersingular reduction of Drinfeld modules*, to appear in Arch. Math., 1999.

[2] *Zeros of Eisenstein series, quadratic class numbers and supersingularity for rational function fields*, to appear in Math. Ann., 1999.

[3] *The 2–primary class group of certain hyperelliptic curves*, preprint 1999.

Coulangeon, Renaud
"*Extreme Humbert forms over algebraic number fields*".

The Hermite's number of a positive definite real quadratic form, which measures the density of the associated sphere packing, is a well–known invariant in the geometry of numbers. As a function on the space of all positive definite quadratic forms in a given dimension n, it attains an absolute maximum γ_n (Hermite's constant). A theorem of Voronoï characterizes quadratic forms at which Hermite's number achieves a local maximum as those which are both *perfect* and *eutactic*.

This classical notion of Hermite's number has been extended to *Humbert–forms* over algebraic number fields by M.I. Icaza and R. Baeza. Among others, the first author gave an explicit bound for the Hermite–Humbert's number of a Humbert form, depending on the field K and the dimension n, and proved that it attains an absolute maximum $\gamma_{n,K}$.

In this talk we characterize *extreme* Humbert forms, *i.e.* those achieving a local maximum of Hermite–Humbert's function, by means of a criterion analogous to Voronoï's theorem, having defined suitable notions of *perfection* and *eutaxy*. We also give an explicit application of this to binary Humbert forms over real quadratic fields.

Daniel, Stephan
"*On the sum of a square and a square of a prime*".

For all positive integers n, let $r(n)$ denote the number of representations of the form $n = m^2 + p^2$, where m and p run through positive integers with p restricted to prime values. Let $E(x)$ denote the number of positive integers $n \le x$ with $r(n) > 0$. In 1968, Rieger proved that

$$\sum_{n\le x} r(n)^2 \ll \frac{x}{\log x}\,. \tag{1}$$

As a corollary, he deduced that

$$E(x) \ge c\,\frac{x}{\log x}$$

holds with some (small) absolute $c > 0$; note that the upper bound $E(x) \le (\frac{\pi}{2} + o(1))\frac{x}{\log x}$ is an easy consequence of the prime number theorem. We improve upon (1) by establishing the asymptotic formula

$$\sum_{n\le x} r(n)^2 = \left(\frac{\pi}{2} + \frac{9}{4}\right)\frac{x}{\log x} + O\left(\frac{x(\log\log x)^2}{(\log x)^2}\right).$$

As a consequence, we deduce the explicit lower bound

$$E(x) \ge \left(\frac{\pi}{3} - \frac{3}{8} - \varepsilon\right)\frac{x}{\log x} \qquad \text{for } x \ge x_0(\varepsilon).$$

The proof requires a weak version of the Barban–Davenport–Halberstam theorem and standard results from sieve theory; apart from this, the proof is essentially elementary. We also mention some results of similar type that can be proved by the same method.

Darmon, Henri
"*Modularity of hypergeometric abelian varieties*".

I will explain how the approach introduced by Wiles for proving the modularity of elliptic curves can be extended to prove the modularity of a class of abelian varieties, whose periods are related to values of classical hypergeometric functions.

Davis, Simon

"*Mathematical Applications of String Theory: Spin Structures on Riemann Surfaces and the Perfect Numbers*".

The equality between the number of odd spin structures on a Riemann surface of genus g, with $2^g - 1$ being a Mersenne prime, and the even perfect numbers, is an indication that the action of the modular group on the set of spin structures has special properties related to the sequence of perfect numbers. A primality test for Mersenne primes is developed by using a geometrical representation of these numbers. The related problem of the non–existence of finite odd perfect numbers is shown to be dependent on the irrationality of the square root of twice the product of a sequence of repunits. Using the characteristics of prime of repunits, it is demonstrate that these products are not equal to twice the square of a rational number.

Deschamps, Bruno

"*Groupe de Brauer des clotures totalement reelles*".

Si $\mathbb{K}$ designe un corps ordonnable, la cloture totalement reelle de $\mathbb{K}$ est le sous–corps de $\overline{\mathbb{K}}$ laisse fixe par les involution de $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ (qui representent en fait tous les elements de torsion de ce groupe). On la note $\mathbb{K}^{\mathrm{tr}}$. Nous montrons que le groupe de Brauer de ce corps est toujours un 2–groupe abelien elementaire. Dans cet expose, nous expliciterons ce groupe dans certain cas particulier comme $\mathbb{K} = \mathbb{Q}$ ou $K = \mathbb{R}((X_1))\dots((X_n))$

Dietmann, Rainer

"*Small solutions of quadratic diophantine equations*".

We consider quadratic diophantine equations, which take the shape

$$Q(x_1, \dots, x_s) = 0 \tag{1}$$

for $Q(X_1, \dots, X_s) \in \mathbb{Z}[X_1, \dots, X_s]$ of degree at most 2. The problem we are concerned with is to provide a 'search bound' for equations of this type. A search bound is a function $f : \mathbb{Z} \mapsto \mathbb{R}_+$ with the property that whenever (1) has an integral solution $\mathbf{x} = (x_1, \dots, x_s)$ at all, then it has one with

$$|x_i| \leq f(H) \quad (1 \leq i \leq s),$$

where $H > 1$ is an upper bound for the absolute values of the coefficients of Q. For convenience assume that the homogeneous quadratic part of Q is non-singular. It has been proved by Kornhauser that we can take

$$f(H) = \begin{cases} C_1(14H)^{5H} & \text{when } s = 2 \\ C_2(s)H^{51H} & \text{when } s \geq 5, \end{cases} \tag{2}$$

where the exponential dependence on H is essentially best possible for $s = 2$. So far very little has been known about the remaining cases $s = 3$ and $s = 4$, and in particular it was not clear if one could get polynomial bounds in H like those for $s \geq 5$. By using a variety of different methods (Hardy-Littlewood circle method, geometry of numbers, automorphs of ternary quadratic forms) we were able to tackle the remaining cases $s = 3, 4$, obtaining the polynomial bounds

$$f(H) = \begin{cases} C_3 H^{100} & \text{when } s = 4 \\ C_4 H^{30000} & \text{when } s = 3. \end{cases}$$

In addition, we could quite substantially improve the result in (2) when $s \geq 5$.

Doche, Christophe
"*On the Spectrum of the Zhang–Zagier Height*".

In this paper we study the Zhang–Zagier height. We know that their height $\mathfrak{H}(\alpha)$ is bounded away from 1 for every algebraic number α different from $0, 1, 1/2 \pm \sqrt{-3}/2$. The study of the related spectrum is especially interesting, for it is linked to Lehmer's problem and to a conjecture of Bogomolov. After recalling some definitions, we show an improvement of the so-called Zhang–Zagier inequality. To achieve this, we need some algebraic numbers of small height. So, in the third section, we describe an algorithm able to find them and we give an algebraic number with height $1.2875274\ldots$ discovered in this way. This search up to degree 64 suggests that the spectrum of $\mathfrak{H}(\alpha)$ may have a limit point less than 1.292. We prove this fact in the fourth part.

Douai, Jean–Claude
"*Corps des modules, Corps de définition et Cohomologie*".

Ceci est le fruit d'un travail en commun avec Pierre Dèbes et de discussions avec M. Emsalem qui s'inscrivent dans la lignée de travaux classiques sur l'existence de solutions de certains problèmes diophantiens dûs à Moret–Bailly, Pop, Green, Roquette. On sait que Q^{tr} (resp. Q^{tp}) est un corps pseudo–réel clos (resp. pseudo–p–adiquement clos) i.e. toute variété lisse, absolument irréductible, définie sur Q admet un point Q^{tr}–rationnel (resp. Q^{tp}–rationnel) si et seulement si elle admet un point réel (resp. un point p–adique). En particulier, $Q^{tr}(\sqrt{-1})$ est P.A.C., donc de dimension cohomologique virtuelle ≤ 1.

D'un autre côté, Flycker, Scheiderer et Sujatha (F.S.S.) ont établi que si K est un corps de dimension cohomologique virtuelle ≤ 1, par exemple si $K = Q^{tr}$, L un K–lien localement représentable par un groupe algébrique, alors l'application $H^2(K, L) \to \Pi_\xi H^2(K_\xi, L)$, ξ décrivant les ordres de K, est injective. Utilisant la généralisation de Moret–Bailly, nous montrons l'analogue du résultat de (F.S.S.) pour $K = Q^{tp}$.

Spécialisant notre résultat aux champs de Hurwitz i.e. aux champs algébriques de modules de G–revêtements de $\mathbb{P}^1$ (G=groupe fini) et plus précisément aux gerbes de Hurwitz que nous avons introduites précédemment et considérées également par Wewers, nous pouvons en déduire qu'un G–revêtement de corps des modules Q admet un modèle défini sur Q^{tp} si et seulement si il admet un modèle défini sur Q_p c'est–à–dire si p est un bon premier. Cela répond positivement à une question de Dèbes–Harbater. Le résultat s'étend au cas des revêtements non nécessairement galoisiens si l'on veut bien utiliser les résultats de M. Emsalem.

Dujella, Andrej
"*A parametric family of elliptic curves*".

Let $k \geq 3$ be an integer and let E_k be the elliptic curve given by

$$E_k: \qquad y^2 = ((k-1)x+1)((k+1)x+1)(4kx+1).$$

It is proven that if $\operatorname{rank}(E_k(\mathbb{Q})) = 1$ or $k \leq 1000$, then all integer points on E_k are given by

$$(x, y) \in \{(0, \pm 1),\ (16k^3 - 4k, \pm(128k^6 - 112k^4 + 20k^2 - 1))\}.$$

The same result is also proven for two subfamilies with rank equal 2 and for one subfamily with rank equal to 3.

Edixhoven, Bas
"*On the Oort–André conjecture*".

The conjecture in question says, roughly, that the irreducible components of Zariski closures of sets of complex multiplication points in moduli spaces of abelian varieties are sub–Shimura varieties. In the talk, we will treat two cases of this conjecture, assuming the generalized Riemann hypothesis for number fields. These two cases concern the moduli space of n-tuples of elliptic curves for arbitrary n, and the moduli spaces of abelian surfaces with endomorphisms by a real quadratic fields (Hilbert modular surfaces). This last case has an interesting application (actually without having to assume GRH) to transcendence of special values of hypergeometric functions via work of Wolfart and Cohen.

For more details and for references, I recommend section 6 of:

B.J.J. Moonen. Models of Shimura varieties in mixed characteristic. Durham proceedings. In: Galois representations in arithmetic algebraic geometry, ed. A. J. Scholl and R. L. Taylor. Cambridge University Press 1998, 267–350.

Elsholtz, Christian
"*A Combined Large Sieve Method and Applications to the Additive Decomposition of the Set of Primes*".

In sieve theory one can usually sift out a small number of residue classes modulo primes. The large sieve method was developed to deal with problems where a large number of residue classes can be sifted.

In this talk we show that a combination of Montgomery's large sieve method and of Gallagher's larger sieve can be used in applications with two sequences. The method allows to sift out *all* residue classes, some in the first sieve process for the first sequence, the others in the second process when sifting the second sequence.

As an interesting application we consider an old problem of Ostmann: Do there exist sets $\mathcal{A}, \mathcal{B}$ of positive integers with $\mid \mathcal{A} \mid, \mid \mathcal{B} \mid \geq 2$ such that $\mathcal{A}+\mathcal{B} := \{a+b, a \in \mathcal{A}, b \in \mathcal{B}\}$ coincides with the set of primes from some point onwards?

The existence of such a decomposition of the set of primes (the inverse Goldbach problem) would have far reaching consequences towards the prime k-tuple conjecture for large k. It is an open question whether such a decomposition exists or not. Previously the strongest known bounds on the counting functions $\mathcal{A}(x) := \sum_{a \leq x} 1$ were (for positive constants c_i)

$$\exp\left(c_1 \frac{\log x}{\log_r x}\right) \ll \mathcal{A}(x) \ll \frac{x}{\exp\left(c_2 \frac{\log x}{\log_r x}\right)}.$$

(Here $\log_r x$ is the r-th fold logarithm. The result with $r=2$ is due to Hofmann and Wolke, and for arbitrary r this is a result of the author.)

Our new methods allows to improve this to

$$x^{\frac{1}{2}}(\log x)^{-C_1} \ll \mathcal{A}(x) \ll x^{\frac{1}{2}}(\log x)^{C_2}.$$

Here C_1, C_2 are small positive constants. The same bounds hold for $\mathcal{B}(x)$.

We conclude with some general remark on the prime k-tuple conjecture for large k.

Fainsilber, Laura
"*An injectivity result for hermitian forms over local orders*".

Let Λ be a ring endowed with an involution $a \mapsto \tilde{a}$. We say that two units a and b of Λ fixed under the involution are *congruent* if there exists an element $u \in \Lambda^\times$ such that $a = ub\tilde{u}$. We denote by $\mathcal{H}(\Lambda)$ the set of congruence classes. This $\mathcal{H}(\Lambda)$ corresponds to a set of isometry classes of hermitian forms.

We consider the case where Λ is an order with involution in a semisimple algebra A over a local field and study the question whether the natural map $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ induced by inclusion is injective. We give sufficient conditions on the order Λ for this map to be injective (for instance that Λ be hereditary). We give applications to hermitian forms over group rings and G–hermitian forms over local rings for certain finite groups G, not necessarily abelian.

Francini, Paolo
"*The function h^o for quadratic number fields*".

Van der Geer and Schoof have recently introduced the notion of "effectivity" of an Arakelov divisor over a number field F, which is a real number in $[0,1]$ attached to it. With this notion, they define a function h^o which yields an exact analogue of Riemann–Roch theorem in the arithmetic case. Here we show that, if F is a quadratic field, the function h^o, restricted to zero-degree divisors over F, attains its maximum for principal Arakelov divisors. This was claimed by a conjecture they made.

Fukuda, Takashi & Komatsu, Keiichi
"*On Iwasawa λ_3–invariants of certain cyclic cubic fields*".

Let k be a cyclic cubic field in which 3 splits, k_n the n–th layer of the cyclotomic $\mathbb{Z}_3$–extension of k, A_n the 3–part of the ideal class group of k_n, B_n the subgroup of A_n consisting of elements which are invariant under the action of $G(k_n/k)$ and D_n the subgroup of B_n generated by ideal classes of prime ideals lying over 3. According to Greenberg's pioneering works, $|B_n|$ increases monotonously and has an upper bound. Moreover, if $B_n = D_n$ for all sufficiently large n, then $\mu_3(k) = \lambda_3(k) = 0$. On the other hand, Ozaki and Yamamoto recently gave a necessary and sufficient condition for $A_1 = D_1$ which also implies $\mu_3(k) = \lambda_3(k) = 0$.

In this talk, we introduce a method of computing $|D_2|$ for k of prime conductor which does not satisfy $A_1 = D_1$. For example, let k be the cyclic cubic field of conductor 9901. Then $|A_1| = 27$ and $|D_1| = 3$. Moreover we have $|B_n| = 9$ for all $n \geq 2$ by Inatomi's theorem. Let $f = 27 \cdot 9901$ and

$$\omega = N_{\mathbb{Q}(\zeta_f)/k_2}(1-\zeta_f)\,.$$

Then ω is a cyclotomic unit of k_2. We define ω_{ij} to be $\omega^{\sigma^i\gamma^j}$, where σ and γ are automorphisms of $k_2/\mathbb{Q}$ defined by $\zeta_{9901}^{\sigma} = \zeta_{9901}^2$, $\zeta_{27}^{\sigma} = \zeta_{27}$, $\zeta_{9901}^{\gamma} = \zeta_{9901}$, $\zeta_{27}^{\gamma} = \zeta_{27}^2$. We construct a unit ε of k which is also cyclotomic unit such that $\{-1, \varepsilon, \varepsilon^{\sigma}\}$ generates the full unit group of k. Then we found that

$$\varepsilon^3\omega_{0,0}^8\omega_{0,1}^4\omega_{0,3}^5\omega_{0,4}^{-2}\omega_{1,0}^{-2}\omega_{1,1}^{-1}\omega_{1,2}^{-3}\omega_{1,3}\omega_{1,4}^{-1}\omega_{1,5}^3\omega_{2,1}^{-3}\omega_{2,2}^3\omega_{2,4}^3\omega_{2,5}^{-3}\omega_{0,6}^2\omega_{1,6}^4\omega_{0,7}\omega_{1,7}^{-1}$$

is 9–th power in k_2 by using computer. From this, we conclude that $N_{k_2/k}(E_2) = E_0^3$ and hence $|D_2| = 9$, where E_n denotes the unit group of k_n. Therefore we have $\mu_3(k) = \lambda_3(k) = 0$ by Greenberg's theorem and Inatomi's theorem.

We can determine $N_{k_2/k}(E_2)$ if we get a subgroup of E_2 with index prime to 3. But a naive method needs 3^{26} trials because k_2 is totally real field of degree 27. This is impossible for computers of the present day. On the other hand, our method needs only 3^{16} trials which is a reasonable number for our computer. Indeed we were able to compute $|D_2|$ within 6 minutes. We can apply our method also for k's of conductors 3907, 4933, 6247, 7687 and 9001.

Gaál, István
"*Power integral bases in algebraic number fields*".

Let K be an algebraic number field of degree n with ring of integers $\mathbb{Z}_K$. It is a classical problem in algebraic number theory to decide if K admits a **power integer basis**, that is an integer basis of the form $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

If $\{1, \omega_2, \ldots, \omega_n\}$ is any integer basis of K, then $D_{K/Q}(X_2\omega_2 + \ldots + X_n\omega_n) = (I(X_2, \ldots, X_n))^2 D_K$ where $I(X_2, \ldots, X_n)$ is the **index form** corresponding to the above integer basis and D_K is the discriminant of K. The element $\alpha = x_1 + \omega_2 x_2 + \ldots + \omega_n x_n \in \mathbb{Z}_K$ generates a power integral basis if and only if

$$I(x_2, \ldots, x_n) = \pm 1$$

Hence the problem of determining power integral bases can be reduced to the resolution of the above **index form equation**.

If K is a cubic number field, the index form equation is a cubic Thue equation, this case was considered by I.Gaál and N.Schulte.

Quartic number fields were studied by I.Gaál, A.Pethő and M.Pohst who showed, that in this case the index form equation can be reduced to a cubic Thue equation and to some corresponding quartic Thue equations.

For quintic fields I.Gaál and K.Győry gave a feasible algorithm for the resolution of the index form equation solving the corresponding unit equation by applying Wildanger's enumeration.

For higher degree number fields, the problem becomes more difficult because of the high degree and the number of variables in the index form equation. The problem is somewhat easier if K has some proper subfields which implies the factorization of the index form.

Sextic and octic fields with a quadratic subfield were investigated by I.Gaál and M.Pohst. Some fields of degree nine that are composits of cubic subfields were studied by I.Gaál.

The talk gives a survey about recent results in this area.

Gallardo, Luis
"*Identities and sums of cubes in* $\mathbb{F}_{2^n}[t]$.".

If a polynomial $P \in \mathbb{F}[t]$ is a sum of n cubes of degree $< \deg(P) + 3$, we say that P is a restricted sum of n cubes. Using identities we prove that every polynomial P in $\mathbb{F}_{2^n}[t]$ is a restricted sum of 9 cubes for all $n \notin \{1, 2, 4\}$., and is a restricted sum of 10 cubes for $n = 4$. Furthermore we prove that if $n \neq 2$ for every polynomial P in $\mathbb{F}_{2^n}[t]$ there exists a square C with $\deg(C) < \deg(P) + 2$ such that $P + C$ is a a restricted sum of 4 cubes.

References:

[1] Car M. et Cherly J., *Sommes de cubes dans l'anneau* $\mathbb{F}_{2^h}[X]$, Acta Arith. **65**, Number 3, (1993) 227–241.

[2] Gallardo L., *Une variante du problème de Waring sur* $\mathbb{F}_{2^n}[t]$. C. R. Acad. Sci. Paris, t.**327**, Série I, (1998) 117–121, 1998.

[3] Lidl R. et Niederreiter H., Finite Fields p. 327 and p. 295. Cambridge University Press 1984.

[4] Vaserstein L.N., *Sums of cubes in polynomial rings,* Math. of Comp. **56**, n^o 193, (1991) 349–357.

Gardeyn, Francis
"*Action of inertia and image of Galois on the torsion of Drinfeld modules*".

Take the ring A of functions on a smooth curve C over a finite field which are regular outside a fixed point. We studied how, for an Drinfeld A–module ϕ defined over a finite seperable extension K of $k(C)$, the representations of the local absolute Galois groups $\mathrm{Gal}(K_\pi^{sep}/K_\pi)$ on the Tate–module $T_v(\phi)$ at primes v of A can be unraveled: the dominant components of this 'dévissage' consist at a finite level of the action on a finite flat subscheme of torsion and on Drinfeld A–lattices. We have tried to describe the action of tame and wild inertia and the size of the image of Galois and of the different as precisely as possible.

Further, we were able to show that, for a rank 2–Drinfeld A–module ϕ over K with $End_{K^{sep}}(\phi) \cong A$, the image of

$$\prod_{v \in \operatorname{Spec} A} \rho_v : \mathrm{Gal}(K^{sep}/K) \to \prod_v \mathrm{GL}_2(A_v)$$

is open.

Gasbarri, Carlo
"*Roth Theorem on non rational ruled surfaces*".

We will speak about a joint work with M. McQuillan "Roth Theorem on non rational ruled surfaces" where we proved the vojta conjecture in some cases namely we proved

Theorem. *Let C be an elliptic curve over K and $p : X \to C$ be a minimal ruled surface; let D be an reduced, effective divisor on X, all of which geometrically irreducible components are either vertical fibers of p or curves which are étale (via p) over C; let H be an ample line bundle on X and $\epsilon > 0$ a real number. Then, there exists a proper (Zariski) closed subset $Z \subset X$ such that, for all $x \in (X \setminus Z)(K)$*

$$m_D(x) + h_{K_X}(x) \leq \epsilon h_H(x) + O(1).$$

we will show then applications to approximations to algebraic numbers

Gee, Alice
"*Special values of modular units*".

We use class field theory to determine radical expressions for certain modular units evaluated at imaginary quadratic numbers. These prove some of Ramanujan's identities found in his Lost Notebook, and allow us to evaluate the Rogers–Ramanujan continued fraction at special points.

Our modular units also yield explicit values for cubic singular moduli which provide power series which converge rapidly to π. This is joint work with Heng Huat Chan and Victor Tan.

Gittenberger, Bernhard
"*Asymptotic Normality of Additive Functions in Number Fields*".

We consider the asymptotic behavior of additive functions f with respect to a canonical number system in a number field. Using exponential sum methods we get a normal limit law for $f(P(z))$ where $P(z)$ is a polynomial with integer coefficients, the leading term of which is positive.

González, Josep & Lario, Joan–C.
"*Manin constants for $\mathbb{Q}$–curves*".

For modular elliptic curves over $\mathbb{Q}$, a certain constant c (constant of Manin) is attached to a representative (minimal model of a strong Weil curve) in their isogeny class. In a running version of a joint paper with Josep González Rovira, we attached a constant c to every isogeny class of modular $\mathbb{Q}$–elliptic curves and predict its value in terms of discriminants and norms. A set of examples are provide to give a glimpse of numerical evidence.

Groenewegen, Richard
"*Arithmetic analogues of theorems for curves*".

A *metrized line bundle* over the ring of integers R of a number field is a projective R–module Λ of rank 1 together with an inner product on the $\mathbb{R}$–vector space $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$. These are arithmetic analogues of divisors on curves. After Van der Geer and Schoof, we define the size $h^0(\Lambda)$ of a metrized line bundle Λ as $h^0(\Lambda) = \log \sum_{x\in\Lambda} e^{-\pi\langle x,x\rangle}$. It is the analogue of the dimension $l(D)$ of the vector space consisting of the functions f for which $(f) + D$ is an effective divisor. With a suitable definition for the degree of a line bundle and a canonical metrized line bundle κ, the Riemann–Roch formula for number fields reads $h^0(\Lambda) - h^0(\kappa\Lambda^{-1}) = \deg \Lambda - \frac{1}{2} \deg \kappa$.

For a divisor D on a curve we have $l(D) = 0$ if its degree $\deg D$ is negative, and Clifford's theorem gives $l(D) < \frac{1}{2}\deg D$ if $\deg(D)$ is within given bounds. We cannot simply replace l by h^0 and D by Λ and get valid formulas in the number field case. In this talk we consider what the analogues of these theorems should be.

Guàrdia, Jordi
"*Arakelov computations in genus 3 curves*".

Arakelov invariants of arithmetic surfaces are well known for genus 1 and 2 ([2], [1]). We study the modular height h and the self–intersection ω^2 of the canonical sheaf for a family of curves of genus 3 with many automorphisms:

$$C_n : Y^4 = X^4 - (4n-2)X^2Z^2 + Z^4.$$

Arakelov calculus implies both analytic and arithmetic computations. We express the periods of the curve C_n in terms of elliptic integrals. The substitutions used in this integrals provide a splitting of the jacobian of C_n as a product of three elliptic curves. Using the corresponding isogeny, we determine the stable model of the arithmetic surface given by C_n.

Once we have the periods and the stable model of C_n, we can study the values $h(C_n)$ and ω^2. We can give a good estimate for the modular height, which reflects the logarithmic behaviour of the height. For the self-intersection ω^2 we give an expression in terms of the Green function and the arithmetic of the curves C_n. We also provide a lower bound, that shows that it is possible to find infinitely many curves with ω^2 as big as desired.

References:

[1] Bost, J. B., *Fonctions de Green–Arakelov, fonctions thêta et courbes de genre* 2, C.R. Acad. Sci. Paris, t. **305**, Série I, (1987) pp. 643–646.

[2] Faltings, G., *Calculus on arithmetic surfaces*, Ann. of Math., **119**, (1984), pp. 387–424.

[3] Guàrdia J., *Geometria aritmètica en una família de corbes de gènere* 3, Thesis, Universitat de Barcelona (1998).

Gusev, Hermann
"*Lemma on isometric linearization and its applications*".

Let $\langle \mathbf{k}, |.| \rangle$ be a locally compact non–archimedean field with nontrivial non–archimedean norm $|.|$, where the characteristic of $\mathbf{k}$ is equal to 0; π be a primitive element of $\mathbf{k}$; $|\pi| = \rho$; $\mathbf{V}$ be the ring of integers of $\mathbf{k}$.

We denote a multiplicative group of unimodular matrices of the n–th order by $UM_n(\mathbf{V})$ and write $U = (u_{ij}) \in UM_n(\mathbf{V})$ if and only if: 1) $\forall i, j : \quad u_{ij} \in \mathbf{V}$; 2) $\det U \in \mathbf{E}$.

Let $X = (x_1, \ldots, x_n)$, $\quad \|X\| = \max_{1 \le i \le n} |x_i|_*$ and $\overline{f}(X) = \overline{f}(x_1, \ldots, x_n) =$ $(f_1(X), \ldots, f_n(X))$,

$$f_i(x_1, \ldots, x_n) = \sum_{\alpha_1 \ge 0, \ldots, \alpha_n \ge 0} c_{\alpha_1, \ldots, \alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n} \tag{1}$$

where $c_{\overline{\alpha}} \in \mathbf{V}$, $\quad \lim_{|\overline{\alpha}| \to +\infty} |c_{\overline{\alpha}}|_* = 0$, $\quad |\overline{\alpha}| = \alpha_1 + \cdots + \alpha_n$.

Lemma (on isometric linearization). *Let $\overline{F}(X)$ be an analytic vector–function with components F_i, of the form (1), $X^0 = (x_1^0, \ldots, x_n^0) \in \mathbf{V}^n$, such that the matrix of Jacobi $MJ_{X^0}(\overline{F}^t) = \left(\frac{\partial F_i}{\partial x_j}\right)\Big|_{X=X^0}$ has an* *inverse. We denote by $\nu_1, \dots, \nu_n$ the system of $UM_n(\mathbf{V})$–invariant exponents of this matrix, $0 \leq \nu_1 \leq \cdots \leq \nu_n$. Then for all $\nu \geq \nu_n + 1$ there is an isometric equivalence*

$$\overline{F}^t(X) \simeq \overline{F}^t(X^0) + MJ_{X^0}(\overline{F}^t)(X - X^0)^t$$

at the compact $K_\nu = K(X^0, \rho^\nu)$.

Corollary (the solvability criterion). Suppose $\overline{F}$ and X^0 are the same as in lemma. Then the system of equations $\overline{F} = \overline{0}$ has a solution on compact K_ν if and only if has a solution the system of equations $L_{X^0}\overline{F}^t(X) = \overline{0}^t$.

The solvability criterion make possible to receive a modification Hensel's lifting lemma on lifting a solution of a congruence system.

References:

[1] Jean–Pierre Serre: *Lie algebras and Lie groups.* N–Y.,1965.

[2] J.P.Bezivin: *Systems d'equations analitytiques. d'apres G. I. Gusev.* Groupe d'etude d'Analyse ultrametrique. 5–e annee. 1977/78, N 5, p. 5/1– 5/5.

Hanrot, Guillaume
"*A new criterion for Catalan's equation*".

In this talk we shall prove by elementary means (i.e., without use of the theory of linear forms in logarithms) that if (p, q) is a pair of primes with $p < q$ and q does not divide the first factor of the class number of the p–th cyclotomic field, then Catalan's equation $x^p - y^q = 1$ has no solution with $|x|, |y| > 1$. Though this criterion is in general weaker than the classical Inkeri–Mignotte–Schwarz one, it happens that the former applies whereas the latter fails.

The proof rests on an elementary method (which follows an idea of Bilu) which allows one to obtain a good bound for the solutions. We shall discuss the (rather strong) conditions under which this method applies.

This is a joint work with Yann Bugeaud.

Harari, David
"*Weak approximation on non simply–connected algebraic varieties*".

Let k be a number field. For any place v of k, denote by k_v the completion of k at v (for example, if k is the field $\mathbb{Q}$ of rational numbers, then the completions are the p–adic fields and the field of real numbers). Let X be a projective and non–singular algebraic variety defined over k with $X(k) \neq \emptyset$. One says that X satisfies *weak approximation* if the set $X(k)$ of k–rational points of X is dense in the product $\prod_v X(k_v)$ (which is equipped with the product of v–adic topologies). Let $\bar{k}$ be an algebraic closure of k and $\overline{X} = X \times_k \bar{k}$.

We show that if the geometric étale fundamental group $\pi_1(\overline{X})$ is not trivial, then X does not satisfy weak approximation. More precisely, we show that under some assumptions, the condition that $\pi_1(\overline{X})$ is not abelian implies that the Brauer–Manin obstruction to weak approximation (this is a cohomological obstruction, related to the Brauer group of X, which for some time explained all counter–examples to weak approximation) is not the only one. For example this statement holds for any bielliptic surface.
(see `http://www.-irma.u-strasbg.fr/irma/publications/1998/98033.shtml` for a preprint about this work).

Henniart, Guy

"*Recent progress on the Langlands conjectures for GL(N)*".

Hill, Richard

"*Metaplectic groups and the Gauss–Schering Lemma*".

Let k be a global field of positive characteristic and let A be its Adele ring. Suppose k contains a primitive n-th root of unity and let μ_n be the group of n-th roots of unity in k. The group $GL_n(A)$ has an n–fold metaplectic extension, that is a topological central extension

$$1 \to \mu_n \to \widetilde{GL}_n(A) \to GL_n(A) \to 1,$$

which splits over the subgroup $GL_n(k)$. I will describe an explicit cocycle corresponding to this extension and give a direct proof that the cocycle is trivial on $GL_n(k)$.

Honsbeek, Mascha

"*Denesting certain nested radicals of depth two*".

As for many subjects in mathematics, the history of denesting nested radicals leads us to Srinivasa Ramanujan (1887–1920). He published the following intriguing equations:

$$\sqrt{\sqrt[3]{5}-\sqrt[3]{4}} = \tfrac{1}{3}\left(\sqrt[3]{2}+\sqrt[3]{20}-\sqrt[3]{25}\right),$$

$$\sqrt{\sqrt[3]{28}-\sqrt[3]{27}} = \tfrac{1}{3}\left(\sqrt[3]{98}-\sqrt[3]{28}-1\right).$$

In one of his notebooks we find a theorem explaining these equations.

Theorem. *If m, n are arbitrary, then*

$$\sqrt{m\sqrt[3]{4m-8n}+n\sqrt[3]{4m+n}} = \pm\tfrac{1}{3}\left(\sqrt[3]{(4m+n)^2}+\sqrt[3]{4(m-2n)(4m+n)}-\sqrt[3]{2(m-2n)^2}\right).$$

We say we have denested the left hand sides of the above equations over $\mathbb{Q}$, since we have replaced expressions involving rational numbers with nesting depth two by expressions consisting of single radicals over $\mathbb{Q}$.

Given a nested radical A over $\mathbb{Q}$ three important questions arise:

1) Can A be denested over $\mathbb{Q}$?

2) If such a denesting of A exists, which radicals will be involved?

3) If a denesting of A exists, how can we determine it?

I will answer these questions for nested radicals of the form $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$, where α and β are rational numbers.

Using elementary results from Galois theory we prove that if a denesting of a nested radical of this form exists, it can be found in the field $\mathbb{Q}(\sqrt[3]{\beta/\alpha}, \sqrt{f})$, for some $f \in \mathbb{Q}$.

We define a polynomial $F_{\beta/\alpha}$ of degree four over $\mathbb{Q}$ and prove that $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$ can be denested over $\mathbb{Q}$ if and only if $F_{\beta/\alpha}$ has exactly one rational root. When we denote this root by n/m, this last condition leads to a theorem that has striking similarities with Ramanujan's theorem.

Theorem. *Let $\alpha, \beta \in \mathbb{Q}^*$, such that β/α is not a cube in $\mathbb{Q}$. The nested radical $\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}}$ can be denested if and only if there exist integers m and n such that*

$$\frac{\beta}{\alpha} = \frac{(4m+n)n^3}{4(m-2n)m^3}.$$

If such integers exist, then the denesting will be

$$\sqrt{\sqrt[3]{\alpha}+\sqrt[3]{\beta}} = \pm\frac{1}{\sqrt{\beta-(n/m)^3\alpha}}\left(-\tfrac{1}{2}(n/m)^2\sqrt[3]{\alpha^2}+n/m\sqrt[3]{\alpha\beta}+\sqrt[3]{\beta^2}\right).$$

Huttner, Marc
"*Equations Différentielles et Approximations Diophantiennes d'Intégrales Abéliennes*".

Les intégrales de Stieltjes suivantes

$$\Psi_i(x) = \Phi(x)^{-1/k}\int_{e_0}^{e_i}\Phi(t)^{-1/k}dt/(x-t), \quad 1 \le i \le m, k \ge 2 \tag{1}$$

où $\Phi(t)$ désigne le polynôme $\prod_{0\le i\le m}(t-e_i)$ à racines distinctes de $\mathbb{Q}[t]$ $(m \ge 2)$, sont en relation avec des intégrales de 3ème espèce sur les courbes hyperrelliptiques $u^k = \Phi(t)$.
Il est facile de trouver des approximations rationnelles simultanées des $\Psi_i(x)$ mais il est beaucoup moins connu qu'en utilisant des propriétés des équations différentielles de Tissot–Pochhammer de leurs adjointes, et un calcul de déterminant de périodes d'intégrales, on peut exprimer les intégrales (1) comme combinaison linéaire d'intégrales abéliennes du type

$$f_i(x) = \Phi(x)^{-1/k}\int_{e_0}^{x} t^{i-1}\Phi(t)^{-1/k}dt \quad 1 \le i \le m \tag{2}$$

(théorème d'échange de l'argument et du paramètre).
Ceci nous permet en particulier d'obtenir des approximations simultanées des intégrales abéliennes (2) et d'en déduire des résultats d'arithmétique nouveaux concernant la nature des intégrales abéliennes $f_i(x)$.

Iwaniec, Henryk
"*Central values of L–functions from analytic view point*".

This lecture will be an overview of recent developments in analytic theory of L–functions which exploit special features of their values at the point of symmetry in the functional equations. Connections with the class number problem, sub–convexity bounds on the critical line, and the Riemann hypothesis for varieties will be discussed.

Kida, Masanari
"*Reduction of elliptic curves over imaginary quadratic fields*".

It is well-known that there is no elliptic curve having good reduction everywhere over the field $\mathbb{Q}$ of rational numbers. This result is further generalized to certain quadratic fields and some other fields.

In this talk, we are particularly interested in the case of imaginary quadratic fields. Setzer and Stroeker (Pacific J. Math. 1978, 1983) prove that there exists no elliptic curve having good reduction at every finite place of an imaginary quadratic field provided the class number of the quadratic field is prime to six.

Setzer also showed a similar non-existence result by using Galois–theoretic property of the field of two-division points.

On the other hand, the only known elliptic curves over imaginary quadratic fields with small discriminants that have good reduction everywhere are the eight curves defined over $\mathbb{Q}(\sqrt{-65})$ found by Setzer.

In this talk, we will extend the above results to other imaginary quadratic fields. Our methods involves

(i) Class number computation of certain quartic number fields,

(ii) Finding integral points in the rings of quadratic integers of certain elliptic curves.

We hope we can find new examples of such elliptic curves defined over imaginary quadratic fields.

Klyachko, Alexander & Kara, Orhun
"*Singularities of The Modular Curve*".

In the work we have described singularities of a natural plane model of the modular curve $X_0(\ell)$ parameterizing cyclic isogenies of degree ℓ of elliptic curves. We have proved that in characteristic $p \neq 2, 3$ and coprime to ℓ the plane projection of $X_0(\ell)$ is immersion everywhere except two cusps. So with these two exceptions all singularities of the plane model are intersections of several smooth branches. It turns out that in non supersingular points there are only two such brunches, while in supersingular points the number of brunches may be arbitrary big. In all three cases we completely determine structure of the singularities.

Let $X_0(\ell)$ be modular curve parameterizing cyclic isogenies $\rho : E \to E'$ of prime degree $\ell = \deg \rho$ of elliptic curves E, E'. The curve $X_0(\ell)$ has singular plane model $Z_0(\ell)$ coming from projection $\pi : X_0(\ell) \to \mathbb{P}^2$ given in affine coordinates by $\rho \mapsto (j(E), j(E'))$. In characteristic $p \neq 2, 3$ the projection π is immersion outside two cusps $0, \infty \in X_0(\ell)$, and near these cusps $Z_0(\ell)$ has singularity analytically equivalent to that of equation $x^\ell = y^{\ell-1}$ at the origin $(0, 0)$.

All other singularities of $Z_0(\ell)$ are intersections of smooth brunches. In characteristic zero these selfintersections are just simple nodes.

The main results are describing singularities of $Z_0(\ell)$ in positive characteristic $p > 3$. Except two cusps they are intersection of smooth brunches passing through point $(E, E') \in Z_0(\ell)$.

As in characteristic zero there are at most two branches through a *non supersingular* point $(E, E') \in Z_0(\ell)$ corresponding to pair of isogenies $\sigma : E \to E'$ and $\rho : E \to E'$. The order of contact of these brunches is equal to p-part of conductor of endomorphism $\alpha = \widehat{\rho}\sigma : E \to E$ (i.e. p-part of index of $\mathbb{Z}[\alpha]$ in ring of integers of imaginary quadratic field $\mathbb{Q}(\alpha)$), where $\widehat{\rho}$ is the dual isogeny of ρ. Let's note that in the case under consideration p necessary splits in $\mathbb{Q}(\alpha)$.

There may be more then two brunches passing through a *supersingular* point $(E, E') \in Z_0(\ell)$. Order of contact of a pair of them, corresponding to isogenies σ, ρ depends on whether p is ramified or remains prime in quadratic field $\mathbb{Q}(\alpha), \alpha = \widehat{\rho}\sigma$. In ramified case the order of contact is equal to

$$2 + 2p + \cdots + 2p^{r-1} + p^r$$

while in unramified case the order of contact is given by

$$2 + 2p + \cdots + 2p^r$$

where p^r is p-part of the conductor of endomorphism $\alpha = \widehat{\rho}\sigma$.

Koike, Kenji
"*The Kuga–Satake varieties attached to double coverings over* $\mathbb{P}^1 \times \mathbb{P}^1$ *branched along four* $(1,1)$*–curves*".

In this talk we construct the Kuga–Satake varieties corresponding to a certain family of polarized $K3$ surfaces. Our family $\mathcal{F}$ is characterized by the transcendental lattice $\mathrm{U}(2)^2 \oplus \langle -2 \rangle$ of rank 8 with the signature $(2, 6)$.

Any generic member of $\mathcal{F}$ can be regarded as a double covering over $\mathbb{P}^1 \times \mathbb{P}^1$ branched along four $(1,1)$ curves (provided a certain fixed polarization). The main result is stated as the following.

Theorem. *For a generic member X of $\mathcal{F}$ the Kuga–Satake variety $KS(X)$ is given by the form*

$$KS(X) \sim (A_1 \times A_2)^4 \quad (\sim \text{ means isogeny}).$$

Where A_i $(i = 1, 2)$ is a 8–dimensional simple abelian variety such that $\mathrm{End}_{\mathbb{Q}}(A_i)$ is equal to the Hamilton quaternion algebra $(-1, -1)_{\mathbb{Q}}$ (over $\mathbb{Q}$).

Moreover, we can obtain the converse in the following sense. The second component A_2 is not isogenous with A_1, but it is determined by A_1. So any abelian variety of the form $(A_1 \times A_2)^4$ becomes to be the Kuga–Satake variety, up to isogeny, for a certain member X of $\mathcal{F}$.

References:

[1] Koike,K. and H.Shiga, *Private notes on double coverings of $\mathbb{P}^1 \times \mathbb{P}^1$ branched along four $(1,1)$–curves.*

[2] Kuga,M. and I.Satake, *Abelian varieties attached to polarized $K3$–surfaces*, Math. Ann. **169** (1967), 239–242.

[3] Satake,I., *Clifford algebras and families of Abelian varieties*, Nagoya Math. J. **27** (1966), 435–466.

Kudryavtsev, Michael
"*The upper estimation of the complete rational exponential sums*".

Let $p > 2$ be a prime, $\alpha \geq 2$ be an integer, $\mathbf{O}_p$ the ring of p–adic integer numbers, $\mathbf{O}_p^n = \mathbf{O}_p \times \cdots \times \mathbf{O}_p$, $F = F(\overline{x}) = F(x_1, \ldots, x_n) = \sum\limits_{i_1 \geq 0} \cdots \sum\limits_{i_n \geq 0} a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n} \in \mathbf{O}_p[x_1, \ldots, x_n]$ be a polynomial.

The modification of Hua's lemma on partition is applied to upper estimating of the complete rational trigonometric sum

$$S = \sum_{1 \leq x_1 \leq p^\alpha} \cdots \sum_{1 \leq x_n \leq p^\alpha} \exp\left(2\pi i \frac{F(x_1 \ldots x_n)}{p^\alpha}\right).$$

Let $F_i = \frac{\partial F}{\partial x_i}$ and $\tau_i = \mathrm{ord}_p\, C(F_i)$, where $C(F_i)$ is a content of the polynomial $F_i(x)$, $(1 \leq i \leq n)$, $\tau_F = \min\limits_{1 \leq i \leq n} \tau_i$, and let

$$H = \sup_{\overline{x} \in \mathbf{O}_p^n} \left\{ \mathrm{ord}_p \left(\det \left(\frac{\partial^2 F}{\partial x_i \partial x_j} \right)_{1 \leq i,j \leq n} \right) \right\} < +\infty.$$

Let $N(\overline{F})$ be a number of solutions on $\mathbf{O}_p^n$ of the system equations

$$F_i(x_1, \ldots, x_n) = 0, \quad 1 \leq i \leq n. \tag{1}$$

If $\overline{\theta} = (\theta_1, \ldots \theta_n)$ is a some solution of this system then let

$$\delta(\overline{\theta}) = \mathrm{ord}_p \left(\det \left(\frac{\partial^2 F}{\partial x_i \partial x_j} \right) \bigg|_{\overline{x} = \overline{\theta}} \right).$$

By δ we denote the maximum $\delta = \max\limits_{\overline{\theta}} \{\delta(\overline{\theta})\}$, where $\overline{\theta}$ pass through all solutions of the system (1).

Theorem. *For all $\alpha \geq 3H - 2\tau_F + 2$ the following estimation is true*

$$|S| \leq N(\overline{F}) p^{\frac{\alpha n + \delta}{2}}.$$

The proof and estimation of $N(\overline{F})$ use the lemmas and statements of the work [1] (in particular the lemma of linearization of the system functions is used).

References:

[1] G.I. Gusev, M.V. Kudryavtsev, V.N. Polyakov, *The isometric method of solution of the systems of congruences and systems of equations in local compact non–archimedean fields*, part 2, Saratov,1998. 23 p.(Deponirovano v VINITI, Moskau.)

Kühnlein, Stefan
"*Families of finite groups*".

There are some families of finite groups which come up in several contexts including number theory, namely: if G is a subgroup of $\mathrm{GL}(n, \mathbb{Z})$, we look at the groups G_p which are the images of G under the natural map to $\mathrm{GL}(n, \mathbb{F}_p)$, where $\mathbb{F}_p$ is the finite field with p elements.

There are some questions which are closely related: a) How does the cardinality of G_p behave in dependance on p?

b) How do G_p and G_q interfere for different primes p and q?

c) What are degrees of generators of $\mathbb{F}_p[X_1, \ldots, X_n]^{G_p}$ as p varies? These are questions having their origin in combinatorial group theory and cohomology of S–arithmetic groups.

It is the aim of this talk to show that and how these properties are related, and to demonstrate that for some groups G, e.g. unit groups in rings of integers embedded in the natural way, they are directly connected with interesting arithmetic properties of number fields.

Kulkarni Manisha V. with Chakraborty K.
"*Solutions of cubic equations in Quadratic Fields*".

Let K be any quadratic field with $\mathcal{O}_K$ its ring of integers. We study the solutions of cubic equations, which represent elliptic curves defined over $\mathbb{Q}$, in quadratic fields and prove some interesting results regarding the solutions by using elementary tools. As an application we consider the Diophantine equation $r+s+t = rst = 1$ in $\mathcal{O}_K$. This Diophantine equation gives an elliptic curve defined over $\mathbb{Q}$ with finite Mordell–Weil group. Using our study of the solutions of cubic equations in Quadratic fields we present a simple proof of the fact that except for the ring of integers of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$, this Diophantine equation is not solvable in the ring of integers of any other quadratic fields, which is already proved in [1]

References:

[1] R. A. Mollin, C. Small, K. Varadarajan and P. G. Walsh, *On unit solutions of the equation $xyz = x + y + z$ in the ring of integers of a quadratic field*, Acta. Arith., **XLVIII**, 341–345 (1987).

Lalande, Franck
"*Une caractérisation des corps de nombres réels engendrés par un nombre de Salem*".

Nous proposons une caractérisation des corps de nombres réels engendrés par un nombre de Salem (c'est à dire par un entier algébrique réel > 1 dont tous les autres conjugués ont un module ≤ 1 avec au moins un conjugué de module 1). Soit K un corps de nombres de degré pair égal à $2n$ et de clôture galoisienne L. Le corps K est engendré par un nombre de Salem si et seulement si K admet $2n-2$ corps conjugués complexes et si le groupe de Galois de l'extension $L/\mathbb{Q}$ est inclus dans le produit en couronne $\mathbb{Z}/2 \wr S_n$.

Plus généralement, un corps de nombres de degré pair non totalement complexe est engendré par un entier algébrique réciproque si et seulement si le groupe de Galois de sa clôture galoisienne est inclus dans $\mathbb{Z}/2 \wr S_n$.

Les démonstrations de ces résultats sont rédigés dans [1].

References:

[1] F. Lalande, *Corps de nombres engendrés par un nombre de Salem*, Acta Arithmetica, **88.2** (1999), 191–200.

Langevin, Michel
"*Equations diophantiennes polynômiales a hautes multiplicités*".

One shows how to write and classify large sets of polynomial relations $A+B=C$ (A,B,C coprime polynomials with integer coefficients) with high multiplicities. Iterative methods generating high multiplicities (semi–simple component of Dunford–Schwartz, Belyi's functions) are developed. Links with Stothers–Mason's Theorem (covering ramified at most in three points: $0, 1, \infty$) and classical conjectures ((abc), M.Hall, M.Hall with radical) are studied.

Lannuzel, Arthur
"*Sur les extensions pro-p-libres d'un corps de nombres algébriques*".

Let k an algebraic number field, $\tilde{K}$ the compositum of all $\mathbb{Z}_p$–extensions of k. Then $\tilde{\Gamma} := \mathrm{Gal}(\tilde{K}/k) \cong \mathbb{Z}_p^{r_2(k)+1+\delta_p(k)}$, where $\delta_p(k)$ is an integer, conjecturally trivial (Leopoldt) and $r_2(k)$ is the number of complex valuations of k. Related with the embedding problem, the natural question is: at which conditions is this $\mathbb{Z}_p$–module the maximal abelian factor group of a free Galois pro–p–group $\mathrm{Gal}(L_{r_2+1}/k)$ of rank $r_2(k)+1$?

More generally:

we call F_d–extension an extension with Galois group isomorphic to F_d, the free pro–p–group with d generators ($d \in \mathbb{N}$).

Let

$$\rho_k = \max\{d \in \mathbb{N} \text{ such that } k \text{ has an } F_d\text{–extension}\}.$$

Assuming Leopoldt Conjecture, we have $\rho_k \leq 1+r_2$, and the preceding question becomes: at which conditions $\rho_k = r_2+1$?

– if k is totally real ($r_2 = 0$), it is obvious that $\rho_k = 1$, and $L_1 = k_\infty^{cycl}$, the cyclotomic $\mathbb{Z}_p$-extension of k.

– if $r_2 \neq 0$, the problem is more difficult and related with some interesting arithmetic properties of k. we know examples where $\rho_k < r_2+1$.

An example with $\rho_k = r_2+1$ is the p-rational fields ([1]), where the Galois of the maximal p-ramified pro-p-extension of k is isomorphic to F_{r_2+1}.

The main result we obtain is, modulo conjectures of the Iwasawa theory proposed by Greenberg, there is not other examples when $\mu_p \subset k$: if $k \supset \mu_p$ with $\rho_k = r_2+1$, then k is p–rational.

References:

[1] A. Movahhedi & . T. Nguyen Quang Do, *Sur l'arithmétiques des corps de nombres p–rationnels.* Séminaire de Théorie des Nombres de Paris, 1987–1988, C. Goldstein ed., @ Birkhauser (1990), 155–200.

Laporta, Maurizio B. S.
"*Some Bombieri–Vinogradov type theorems on the Goldbach–Waring problem*".

Denote by $I_{l,k}(N)$ the number of solutions of $p_1^g + p_2^g + \ldots + p_s^g = N$ in primes such that $p_1 \equiv l (\bmod k)$. I will talk about some Bombieri–Vinogradov type results for $I_{l,k}(N)$, with $g \leq 1$ and some $s = s(g)$.

Lauter, Kristin

“*Geometric Methods for Improving Bounds on the Number of Rational Points on Curves over Finite Fields*”.

This talk will present methods and results for improving the upper bounds on the number of rational points on curves over finite fields. The first bound was discovered in the 1940s by André Weil as a direct result of proving the Riemann Hypothesis for curves. For large genus, Serre introduced the explicit formulae method which leads to vast improvements. I will explain three geometric methods for further improving the bounds and give examples of the improvements obtained. The methods rely on first determining the possible zeta functions for a curve, then applying the ideas of Galois descent, Honda–Tate theory, and arguments on endomorphisms of the Jacobian of a curve.

Lefeuvre, Yann

“*Relative class number one problem for dihedral* CM*–field*”.

Let N a CM–field i.e. a totally imaginary number field quadratic over its maximal totally real subfield N^+. It is known that there are only finitely many normal CM–fields with class number one (see [8]). K. Yamamura (see [9]) found all such N with an abelian Galois group. The aim of this talk is to solve the class number one problem for dihedral CM–field. In fact we solve the relative class number one problem for dihedral CM–field, where the relative class number of N is defined by $h_N^- = \frac{h_N}{h_{N^+}}$. We finally obtain the following result:

Theorem. *There are exactly* 43 *dihedral non–abelian CM–fields with relative class number one, and* 32 *of them have class number one. More precisely:*

1. *(see* [4]*)* 19 *of degree* 8 *and* 17 *of them have class number one;*
2. *(see* [6]*)* 16 *of degree* 12 *and* 9 *of them have class number one;*
3. *(see* [5]*)* 5 *of degree* 16 *and* 4 *of them have class number one;*
4. 2 *of degree* 20 *and* 1 *of them has class number one;*
5. 1 *of degree* 24 *and it has class number one.*

The three main steps to solve this problem are :

1. Construct dihedral fields by using class field theory (see [7]).
2. Find good lower bounds on h_N^- (see [1] and [2]) increasing with d_N the absolute value of the discriminant of N. We obtain $d_N > D$ implies that $h_N^- > 1$. Thus we obtain a short list of N which can have relative class number one.
3. Find an efficient technic for computing h_N^- to solve the problem (see [3]).

References:

[1] S. Louboutin, *Majorations explicites du résidu au point* 1 *des fonctions zêta de certains corps de nombres,* J. Math. Soc. Japan **50** (1998), 57–69.

[2] S. Louboutin, *Upper bounds on* $|L(1,\chi)|$ *and applications,* Canad. J. Math. **50** (1998), 795–815.

[3] S. Louboutin, *Computation of* $L(0,\chi)$ *and of relative class numbers of CM–fields*, Preprint Univ. Caen (1998).

[4] S. Louboutin, R. Okazaki, *Determination of all non–normal quartic CM–fields and of all non–abelian normal octic CM–fields with class number one,* Acta Arith. **67** (1994), 47–62.

[5] S. Louboutin, R. Okazaki, *The class number one problem for some non–abelian normal CM–fields of* 2*–power degrees,* Proc. London Math. Soc.(3) **76** (1998), 523–548.

[6] S. Louboutin, R. Okazaki, M. Olivier, *The class number one problem for some non–abelian normal CM–fields,* Trans. Amer. Math. Soc. **349** (1997), 3657–3678.

[7] S.Louboutin, Y.H. Park, Y. Lefeuvre, *Construction of the real dihedral number fields of degree* 2*p. Applications*, Preprint Univ. Caen (1998).

[8] A.M. Odlyzko, *Some analytic estimates of class numbers and discriminants*, Invent. Math. **29** (1975), 279–286.

[9] K. Yamamura, *The determination of the imaginary abelian number fields with class number one*, Math. Comp. **62** (1994), 899–921.

Lehman, Lerry
"*Computation of L–series values for twists of elliptic curves*".

We demonstrate a procedure for computing L–series values for twists of certain elliptic curves. Let E be an elliptic curve over $\mathbb{Q}$ with rank zero and conductor N such that either N or $N/4$ is squarefree, and let ϕ_E be its weight two newform. Using isogeny invariants of E, we can construct from ternary quadratic forms a weight $3/2$ modular form that is a preimage of ϕ_E under the Shimura correspondence. (This construction has been carried out explicitly for all E as above with $N < 2000$.) In this address, we will demonstrate how these modular forms can be used to compute special L–series values for quadratic twists of E, and describe (conjectural) consequences about those curves under the Birch/Swinnerton–Dyer conjecture.

Lettl, Günter & Pethő, Attila & Voutier, Paul
"*Simple families of Thue inequalities*".

We use the hypergeometric method, which goes back to A. Thue and C.L. Siegel, to obtain effective estimates for the measure of irrationality for certain algebraic integers. These results enable us to obtain effective bounds on the solutions of the following three "simple" families of Thue inequalities

$$|F_t^{(j)}(X,Y)| \le k(t) \ ,$$

where $t \in \mathbb{Z} \setminus T_j$, $j \in \{3,4,6\}$, $k : \mathbb{Z} \to \mathbb{N}$ and

$$\begin{aligned} F_t^{(3)}(X,Y) &= X^3 - tX^2Y - (t+3)XY^2 - Y^3 \\ F_t^{(4)}(X,Y) &= X^4 - tX^3Y - 6X^2Y^2 + tXY^3 + Y^4 \\ F_t^{(6)}(X,Y) &= X^6 - 2tX^5Y - (5t+15)X^4Y^2 - \\ &\quad - 20X^3Y^3 + 5tX^2Y^4 + (2t+6)XY^5 + Y^6 \ . \end{aligned}$$

Here T_j denotes a relatively small set of parameter values, for which this method does not apply, e.g. $T_3 = \{t \in \mathbb{Z} \mid -32 \le t \le 29\}$.

The obtained numerical results are almost always far better than those using lower bounds for linear forms in logarithms. Furthermore, there is no more need to investigate the arithmetic of the underlying number fields (e.g. fundamental units or a set of integers with given small norm).

References:

[1] G. Lettl, A. Pethő and P. Voutier, *Simple families of Thue inequalities*, Trans. Amer. Math. Soc., **351**, 1871–1894 (1999).

Liebendörfer, Christine
"*Heights over division algebras*".

We make a start on the definition and study of heights over division algebras.

The simplest case is that of a positive definite quaternion algebra D over the rationals $\mathbb{Q}$. Let A be a matrix over D with M rows and N columns, and suppose that A has left row rank $M < N$. For an order Ω in D we define the height $H^{\Omega}(A)$ as follows. Multiply A by a positive integer a to get its entries into Ω. Then A can be considered as a right D–linear map from Ω^N into Ω^M, and we write

$$H^{\Omega}(A) = \{\, nr(AA^*) \,/\, [\Omega^M : A(\Omega^N)] \,\}^{1/4}$$

where A^* is obtained from A by transposing and applying the canonical involution to the entries, and nr denotes the reduced norm down to $\mathbb{Q}$. This height does not depend on the multiplying integer a and it coincides with the classical height if A is defined over $\mathbb{Q}$.

We are able to prove natural analogues of the well–known results of Bombieri–Vaaler on upper bounds for solutions of $AX = 0$ with X in Ω^N; and we can also establish analogues of the results of Roy–Thunder on lower bounds.

Lorenzini, Dino
"*On the special fiber of Néron models*".

This is joint work with Qing Liu. Let K be a field with a discrete valuation. Let $\mathcal{O}_K$ denote the ring of integers of K. Let k be the residue field of $\mathcal{O}_K$, assumed to be algebraically closed of characteristic $p \geq 0$. Let G/K be a commutative group scheme with Néron model $\mathcal{G}/\mathcal{O}_K$. Let $\mathcal{G}_k/k$ be the special fiber of $\mathcal{G}/\mathcal{O}_K$, and let $\mathcal{G}_k^0/k$ denote the connected component of 0 in $\mathcal{G}_k$. The group of components of $\mathcal{G}$ is the finite abelian group $\Phi := \mathcal{G}_k/\mathcal{G}_k^0$. In this talk, we shall discuss the group structure of the extension

$$0 \longrightarrow \mathcal{G}_k^0 \longrightarrow \mathcal{G}_k \xrightarrow{c} \Phi \longrightarrow 0.$$

When G has purely additive reduction, this extension is split unless the group G/K achieves semistable reduction after a wildly ramified extension L/K. We shall discuss the case of elliptic curves and of norm tori for cyclic extensions of degree p. In these cases, we find that there exists a constant c depending only on the dimension of G such that, if $\mathcal{G}_k$ is totally not split, then the exponent of the wild conductor of G is bounded by c.

Lorenzon, Pierre
"*Logarithmic Hodge–Witt forms and Hyodo–Kato cohomology*".

We extend some results of Illusie–Raynaud and Bloch–Kato to Hyodo–Kato cohomology. Let S be the spectrum of a perfect field of positive characteristic endowed with a fine and saturated log structure and X a proper, smooth and of Cartier type fine and saturated log scheme over S. The Hyodo–Kato cohomology groups $H^m(X/W(S))$ are endowed with a Frobenius operator. We study the slopes of the corresponding crystals, using their alternative description as the hyper cohomology groups of the De Rham–Witt complex $W_n\Omega^\bullet$. We recall that the the slope spectral sequence degenerates modulo torsion and Mazur–Ogus type results on Newton and Hodge polygons. We also consider logarithmic Hodge–Witt sheaves $W_n\Omega^q_{\log}$ which are in a suitable sens the fixed points of F on $W_n\Omega^q$. We extend structure theorem of Illusie–Raynaud for their cohomology groups. Finally we discuss the notion of ordinariness, generalizing criteria of Bloch–Kato.

Masser, David
"*Intersecting a curve with multiplicative groups*".

Suppose we are given a finite collection of algebraic functions of one variable, and that these functions are multiplicatively independent. Then it seems plausible that their values at most points remain independent, and indeed in 1989 it was proved that the exceptional points are sparse in a strong sense. We discuss recent work of Bombieri, Zannier and the speaker which leads under natural hypotheses to even stronger conclusions including finiteness of the set of points which are "doubly exceptional".

Mignotte, Maurice
"*A survey on recent results on Catalan's equation*".

We consider the results obtained since 1992. These include new algebraic criteria "a la Inkeri", sharpening of upper bounds, huge computation to obtain lower bounds and arithmetical results about the exponents.

Mihăilescu, Preda & Morain, François
"*Certifying Cyclotomy Primality Proof*".

Elliptic curves and cyclotomy are the current main streams for primality proving. While cyclotomy is in practice more performant, it suffers of two major disadvantages with respect to elliptic curve proofs (ECPP). First, the asymptotics of cyclotomy is not polynomial and, second, no other means for verifying a cyclotomy proof is known, other than repeating the same computations done for the proof itself. ECPP, on the other hand, allows building *certificates*, which may be verified very fast.

We give a partial solution for the second problem. In a cyclotomy primality proof of a test number n, one chooses a parameter $s > \sqrt{n}$ such that $t = \mathrm{ord}_s(n) = \mathcal{O}\left((\log n)^{\log\log\log n}\right)$. First one proves the existence of a *cyclotomic extension* ([1], [2], [3]) of order s of $\mathbb{Z}/(n \cdot \mathbb{Z})$. The existence of this extension implies that all possible factors of n are $r \in \langle n \mod s\rangle$. The second part of the proof consists in verifying that no element of the cycle $\langle n \mod s\rangle$ is a non trivial factor of n. We show that it is possible to build a certificate of the first - computation intensive - part of the proof and the verification of this certificate takes a factor of $\log n$ less computations to verify than to build. In practice, the verification of a certificate for a 10000 bit number takes several minutes, while building it requires about a week of CPU time on a modern work station. The means for building the certificates are, in a wider sense, inspired from the classic theory of solving cyclic equations by radicals.

The solution is only partial, since the final part of the proof cannot be certified; this part consists however only of trial divisions which are less prone to errors. The certificates require the possibility of using large data bases of precomputed (and validated) Jacobi sums.

References:

[1] H.W.Lenstra Jr.:, *"Primality Testing Algorithms (after Adleman, Rumely and Williams)"*, Seminaire Bourbaki # 576, Lectures Notes in Mathematics, **vol 901**, pp 243-258

[2] H.W.Lenstra Jr.: *"Galois Theory and Primality Testing", in "Orders and Their Applications*, Lecture Notes in Mathematics, **vol 1142**, (1985) Springer Verlag

[3] Mihăilescu, P.M.: *"Cyclotomy of Rings & Primality Testing"*, dissertation 12278, ETH Zürich, 1997.

Monsurrò, Marina
"*Doubling Trace forms*".

Let k be a field of characteristic $\neq 2$, and let L be a Galois extension of finite degree of k. Let $G = Gal(L/k)$. The trace form

$$q_L : L \times L \to k$$

$$q_L(x,y) = tr_{L/k}(xy)$$

is a non–degenerate symmetric bilinear form. It is also a G–form (that is, it is invariant by the action of G).

The structure of the G–form q_L has been investigated in several papers. If G has odd order, then q_L is always isomorphic to the standard G–form (cfr. [2]). This is no longer true if G has even order. In the special case where the 2–Sylow subgroups of G are elementary abelian or quaternionian, the isomorphism class of the G–form q_L is completely determined by some cohomological invariants (cfr. [6]). However, the problem is still open in general.

Galois extensions with group G are special cases of G–Galois algebras. As the latter setting is more natural and more general, let us adopt it. In this conference, based on a joint paper with my supervisor Eva Bayer–Fluckiger, I consider multiples of trace forms. If m is a positive integer, and q a symmetric bilinear form over k, let us denote by $[m]q$ the orthogonal sum of m copies of q. This point of view is already present in [1] and [3], where some results and conjectures are given concerning multiples of trace forms over certain fields.

Let k_s be a separable closure of k, and let $\Gamma_k = Gal(k_s/k)$. The G–Galois algebra L determines, up to conjugation, a homomorphism $\phi_L : \Gamma_k \to G$. This induces a homomorphism $\phi_L^* : H^1(G,\mu_2) \to H^1(\Gamma_k,\mu_2) \simeq k^*/k^{*2}$. For $x \in H^1(G,\mu_2)$, set $x_L = \phi_L^*(x)$. It is easy to see that the elements x_L are invariants of the isomorphism class of the G–form q_L. Moreover, if the 2–cohomological dimension of Γ_k is at most 1, then it is shown in [6] that they determine the isomorphism class of q_L,

In [1], is conjectured that if the 2–cohomological dimension of Γ_k is at most d, then the isomorphism class of $[2^{d-1}]q_L$ is determined by the values x_L for all $x \in H^1(G,\mu_2)$. Note that for $d=1$, we recover the above mentioned result of [6]. The aim of this conference is to prove this conjecture for $d=2$. More precisely, we have

Theorem. *Suppose that the 2–cohomological dimension of Γ_k is at most 2. Let L and L' be two G–Galois algebras over k. Then the g–forms $[2]q_L$ and $[2]q_{L'}$ are isomorphic if and only if*

$$(x_L,-1) = (x_{L'}) \in H^2(\Gamma_k,\mu_2) \simeq Br_2(k)$$

for all $x \in H^1(G\mu_2)$.

Analogous results are given for fields of virtual 2–cohomological dimension at most 2. The proofs use recent results on the Galois cohomology of linear algebraic groups, established in [4] and [5], and Scheiderer's papers [7] and [8].

References:

[1] E. Bayer–Fluckiger, *Galois cohomology and the trace form, Jahresber.* DMV **96** (1994), 35–55.

[2] E. Bayer–Fluckiger and H.W. Lenstra, *Forms in odd degree extensions and self dual normal bases*, Amer. J. Math. **112** (1990), 359–373.

[3] E. Bayer–Fluckiger and J. Morales, *Multiples of trace forms in number fields*, AMS Proc. Symposia Pure Math., **58**.2 (1995) 73–81.

[4] E. Bayer–Fluckiger and R. Parimala, *Galois cohomology of linear algebraic groups over fields of cohomological dimension* ≤ 2, Invent. Math., **122** (1995) 195–229.

[5] E. Bayer–Fluckiger and R. Parimala, *Classical groups and the Hasse principle*, Ann. of Math. (to appear).

[6] E. Bayer–Fluckiger and J.P. Serre, *Torsions quadratiques et bases normales autoduales*, Amer. J. Math. **116** (1994) 1–64.

[7] C. Scheiderer, *Hasse principles and approximation theorems for homogeneous spaces of virtual cohomological dimension one*, Invent. Math. **125** (1996), 307–365.

[8] C. Scheiderer, *Classification of hermitian forms and semisimple groups over fields of virtual cohomological dimension one*, Manuscr. Math. **89** (1996), 373–394.

Movahhedi, A. Chazad & Kolster, Manfred
"*Bi–quadratic Number Fields with trivial* 2*–primary wild Kernel*".

This is a joint work with Manfred KOLSTER.

Let F be a number field with ring of integers o_F. For a finite or real infinite prime v, let F_v denote the local field at v. Let $\mu(F)$ and $\mu(F_v)$ denote the groups of roots of unity of F and F_v, respectively. The classical wild kernel of F – denoted by $WK_2(F)$ – is by definition the kernel of the map $K_2(F) \to \oplus_v \mu(F_v)$ given by the $|\mu(F_v)|$–th power norm residue symbols at v. Moore's reciprocity law yields an exact sequence

$$0 \to WK_2(F) \to K_2(F) \to \oplus_v \mu(F_v) \to \mu(F) \to 0,$$

where v runs through all finite and real infinite primes of F.

The quadratic number fields $F = \mathbb{Q}(\sqrt{d})$, with trivial 2–primary wild kernels were completely described by Browkin and Schinzel. In the twentieth "Journées Arithmétiques", we presented a genus formula for the p–primary part of the wild kernels where p is a prime number. In the present talk, using this genus formula for $p = 2$, we completely determine all bi–quadratic extensions of $\mathbb{Q}$, which have trivial 2–primary wild kernels.

Moshchevitin, Nikolai
"*M. Hall's theorem and* τ*–sets*".

M. Hall (1947) proved that any real number x can be represented in a form

$$x = a + b + c, \quad or \quad x = ab + c,$$

where a, b are badly approximable numbers and c is an integer. This result has multidimensional generalizations by Cassels, Davenport and others. W. Shmidt introduced the notion of α–winning set and by means of this concept he investigated the Diophantine sets connected with badly approximable numbers.

From another hand S. Newhouse and R. Williams gave generalizations of Hall's result on real line in terms of thickness of a Cantor set.

In my lecture I will show some new generalizations of Hall's theorem. For example I will prove that any real x has a representation in a form $x = G(a, b) + c$, where G is a function in two variables under certain conditions and a, b are badly approximable numbers, I will show that the intersection of two thick τ–sets has a thick τ_1–subset and I will formulate a general theorem on intersections of abstract τ–sets in continuums.

Nakano, Shin
"*A note on the rank of ideal class groups*".

Let p be a prime. For an integer $n > 1$ prime to p, denote by $c(n,p)$ the order of p modulo n, and by $d(n,p)$ the minimum of $c(l,p)$ for all prime factors l of n. For a finite abelian group A, let r_pA be the rank of the Sylow p–subgroup of A; $r_pA = \dim_{\mathbb{F}_p}(A/pA)$. Denote by $C(K)$ and $h(K)$ the ideal class group and the class number of an algebraic number field K.

Let k be an algebraic number field of finite degree and K a Galois extension of k of degree n prime to p. Iwasawa [Nagoya Math. J. 27(1966)] showed the inequality $r_pC(K) \geqq d(n,p)$ in case $p \nmid h(k)$ and $p \nmid h(K)$. This result was deduced from the following group theoretical property which was observed by himself.

Let G be a group of order n prime to p, and M an $\mathbb{F}_p[G]$–module such that the action of G on M is non–trivial. Then $\dim_{\mathbb{F}_p} M \geqq d(n,p)$.

Suppose G and M are as above. Then G acts non–trivially on the quotient module M/M^G, where M^G is the submodule of M consisting of elements left fixed by G. Therefore the conclusion of the above property can be replaced by $\dim_{\mathbb{F}_p} M - \dim_{\mathbb{F}_p} M^G \geqq d(n,p)$. This enables us to improve on the result of Iwasawa. In fact, for a Galois extension K/k as stated above, we can prove that if $r_pC(K) > r_pC(k)$ then $r_pC(K) - r_pC(k) \geqq d(n,p)$.

By the same consideration, we can extend the results of Masley [Compositio Math. 37(1978)], Cornell–Rosen [J. Number Theory 13(1981)] and Cornell [Number theory and applications, NATO adv. Sci. Inst. Ser. C 265(1989)]. There are also some applications to the rank of Mordell–Weil groups of abelian varieties.

Nazarova, Katerina & Gusev, Hermann
"*On isometries in locally compact non–archimedean fields*".

Let $\mathbf{k}$ be non–archimedean locally compact field, $\mathbf{k}^n = \mathbf{k} \times \cdots \times \mathbf{k}$.

In this talk we consider the groups of isometries of the compacts from $\mathbf{k}^n$ and related with it the classes of equivalent functions, which are analytic on these compacts. In these classes the canonical elements (forms) are distinguished, which applied numerous supplements in the Number Theory, in Diohantine analysis and in the theory of additive measure of Haare integration in l–adic fields.

Niederreiter, Harald with Cohen, Stephen. D. & Shparlinski, Igor E. & Zieve, Michael
"*Incomplete Character Sums and a Special Class of Permutations*".

Let G be a finite abelian group of order m and $\mathrm{Sym}(G)$ the group of permutations of G. For a fixed $\pi \in \mathrm{Sym}(G)$ the sequence $u_0, u_1, \ldots$ of elements of G is generated by the recursion

$$u_{n+1} = \pi(u_n) \quad \text{for } n = 0, 1, \ldots .$$

This sequence is purely periodic with least period $t \leq m$. For applications in areas such as pseudorandom number generation it is of great interest to obtain nontrivial bounds for incomplete character sums with arguments u_n, but few results are known in this direction.

Suppose that for some integer $K \geq 2$ the permutation $\pi \in \mathrm{Sym}(G)$ satisfies the condition

$$\pi^k - \iota \in \mathrm{Sym}(G) \quad \text{for } k = 1, 2, \ldots, K-1, \tag{1}$$

where ι is the identity map on G. Then by a new method we can show that for any nontrivial character χ of G we have

$$\left| \sum_{n=0}^{N-1} \chi(u_n) \right| \leq K^{-1/2} N^{1/2} m^{1/2} + \frac{1}{2} K \quad \text{for } 1 \leq N \leq t.$$

For instance, if $1 \leq N \leq t$ and (1) is satisfied with $K \geq N^{1/3} m^{1/3}$, then

$$\left| \sum_{n=0}^{N-1} \chi(u_n) \right| \leq \frac{3}{2} N^{1/3} m^{1/3} + \frac{1}{2}.$$

Permutations π of G satisfying (1) form an interesting subclass of orthomorphisms of G which allows applications to the construction of combinatorial designs. The case where G is the additive group of a finite field $\mathbb{F}_q$ is of special interest. Various permutations π of $\mathbb{F}_q$ satisfying (1) can be constructed, e.g. if π is a linear operator of the vector space $\mathbb{F}_q$ over its prime subfield and the eigenvalues of π are primitive elements of $\mathbb{F}_q$, then (1) holds with $K = q - 1$.

Papanikolas, Matthew A.
"*Gamma Values and Linear Independence in Characteristic p*".

Let $k_\infty = \mathbb{F}_q((1/t))$ be the completion of $k = \mathbb{F}_q(t)$ at ∞, and take $\Gamma(x)$ for Thakur's characteristic p gamma function on $\overline{k}_\infty$, defined by

$$\Gamma(x) = \frac{1}{x} \prod_{n \in \mathbb{F}_q[t]_+} \left(1 + \frac{x}{n}\right)^{-1}.$$

Working jointly with W. D. Brownawell, we use methods from the theory of Drinfeld modules and t-modules, including the soliton approach of Anderson and Sinha, to investigate linear independence criteria over $\overline{k}$ among special values of $\Gamma(x)$ for $x \in \mathbb{F}_q(t)$.

Perret, Marc
"*On the ideal class group problem for global fields*".

Let G be a finite abelian group and q be a prime power. We prove that for infinitely many finite separable extensions K of $\mathbb{F}_q(T)$, the ideal class group of the ring of regular functions outside the infinite places of K is isomorphic to G.

Peyre, Emmanuel
"*Flags of bounded height in the functional case*".

Let F be a global field of finite characteristic and V be a generalized flag variety over F defined as the quotient of a semi-simple group over F by a reduced parabolic subgroup. For particular choices of heights, the corresponding height zeta function defined by

$$\zeta_{H,V}(s) = \sum_{x \in V(k)} \frac{1}{H(x)^s}$$

is an Eisenstein series. Then, using the work of Morris, it is possible to study this height zeta function. In particular if the chosen height corresponds to an adelic metric on the anticanonical line bundle then the height zeta function is holomorphic for $\mathrm{Re}(s) > 1$ and extends to a meromorphic function which has a pole of order t at $s = 1$, where t is the rank of the Picard group of V. Moreover, as in the number field case, the value of the limit

$$\lim_{s \to 1} (s-1)^t \zeta_{H,V}(s)$$

may be expressed in terms of the volume of the adelic space for a Tamagawa measure associated to the given metric.

Poonen, Bjorn
"*Algebraic families of nonzero elements of Shafarevich–Tate groups*".

We construct non–trivial families of torsors of abelian varieties parameterized by an open subset of $\mathbb{P}^1$ over $\mathbb{Q}$ such that every rational fiber (and in fact each fiber above a closed point of odd degree) represents a nonzero element of the Shafarevich–Tate group of the corresponding abelian variety. This is joint work with Jean–Louis Colliot–Thélène.

Popov, Sergei & Valentin Voskrenskii

"*Galois Modules and Models of Algebraic Tori*".

Let G be a connected linear algebraic group over a field of $\wp$–adic numbers k, $\mathcal{O} = \mathcal{O}_k$ a ring of integral elements of k. We call *integral model* of G a group scheme X of finite type over $\mathcal{O}$ such that the condition $X \otimes_{\mathcal{O}} k \;\cong G$ holds. Any exact linear representation of G over k allows us to construct such an integral model. The structure of k–group G does not depend on the choice of the exact representation of G but the structure of integral form really does. However in the case of an algebraic torus T there exists a distinguish integral form X of T such that $X = \operatorname{Spec} A$, where A is determined by the parameters of T only. The form X has some extreme properties. We call this form *canonical* or *minimal* integral model of T.

Theorem 1 *Let T be an algebraic torus, L the minimal split field of T. Then the canonical $\mathcal{O}$–form $X = \operatorname{Spec} A$ of T has the following properties:*

1. $A \subset k[T],\ A \cap k = \mathcal{O},\ k \otimes_{\mathcal{O}} A \cong kA = k[T]$;
2. *A is the Hopf algebra of finite type over $\mathcal{O}$, which induces the initial Hopf algebra structure on $k[T]$;*
3. *the algebra A is a faithfully flat over $\mathcal{O}$;*
4. $f(u) \in \mathcal{O},\ \forall u \in U$ *and* $\forall f \in A,\ X(\mathcal{O}) = U = \operatorname{Hom}_\Pi(\hat{T}, \mathcal{O}_L^*)$;
5. $\mathcal{O}_L[\hat{T}] \subset \mathcal{O}_L A;\ \mathcal{O}_L[\hat{T}] = \mathcal{O}_L A$ *if and only if the extension L/k is unramified.*

We call *the reduction of T modulo $\wp$* the reduction of its canonical integral form. Let F/k be a finite extension, E the maximal unramified extension of the field k in F, $(F : E) = e,\ (E : k) = f$.

Theorem 2 *The reduction $Y_\wp$ of the torus $R_{F/k}(\mathbf{G}_m)$ is a connected algebraic group over the finite field $r_k = O/\wp$. This group is the direct product of the torus $R_{r_F/r_k}(\mathbf{G}_m)$ by a unipotent group $U_\wp$.*

Theorem 3 *The reduction $X_\wp$ of the norm torus $R^{(1)}_{F/k}(\mathbf{G}_m)$ is a product $Z \times_{r_k} U_\wp$, here $U_\wp$ is group from theorem 2, $Z = \operatorname{Spec} A,\ A = r_k[u_1, \dots, u_f]/(z^e - 1)$, here z is the norm form of the extension r_E/r_k. If $\wp$ does not divide e then $X_\wp$ is an algebraic group and if $e > 1$ then $X_\wp$ is not connected; if $\wp$ divides e then $X_\wp$ is not reduced.*

Let T be an arbitrary k–torus and L the minimal split field of T, $k \subset E \subset L,\ \Delta = \operatorname{Gal}(L/E)$. Let also I be the ideal of augmentation of the group ring $\mathbb{Z}[\Delta]$, then we have the submodule $I\hat{T}$. The module $\hat{T}/I\hat{T}$ is a Γ–module and $\Gamma = \Pi/\Delta$ determines the multiplicative part of the reduction $T_\wp$. The unipotent part of $T_\wp$ is determined by the module $I\hat{T}$ but we have no its exact description yet.

Let T be an algebraic k–torus, here k is a field of algebraic numbers. Let also L/k be the minimal split field of T and $\Pi_\wp$ the group of decomposition defined for every prime $\wp$ of the ring $\mathcal{O}$ of integers of the field k, $\Pi_\wp \subset \Pi = \operatorname{Gal}(L/k)$. Using method described above we can construct the canonical model $X_\wp$ of the torus $T \otimes_k k_\wp$. There exists the canonical Haar's measure $\mu_\wp$ on $T(k_\wp)$. In some cases we calculate the exact value $\mu_\wp(X_\wp(\mathcal{O}_\wp))$ for the points $\wp$ of ramification (for unramified points these values are well known and they are equal to the values of the local Artin's L–functions). These calculations allow us to get the exact value of the class number of the adele group $T(A)$ and calculate the local factors of the zeta–function of T in the points of ramification. The existence of an integral basis of any finite extension of the field of rational numbers $\mathbb{Q}$ allows us to construct the global $\mathbb{Z}$–model X of the torus T using this method. The class number of the global model X can be calculated using Tamagawa's numbers and the exact value of the reduction X_p. These models of tori of low dimension are studied.

POULAKIS, DIMITRIOS
"*On the reduction modulo p of absolutely irreducible polynomials*".

Let F be an absolutely irreducible polynomial in $\mathbb{Q}[X_1, \cdots, X_s]$. In 1919, Ostrowski proved that there is a positive integer A such that if p is a prime $\geq A$, then the reduction of F modulo p is an absolutely irreducible polynomial. Several proofs of this result was given but only the proofs of Ruppert (1986) and Zannier (1997) for the case $s = 2$ lead to an explicit upper bound of polynomial type for A. Let K be a number field and O_K as its ring of integers. In this talk we give a quite brief proof of this result for the case of $K[X,Y]$, using a different method which provide an explicit polynomial bound for A. Our method is relied on an effective version of Riemann–Roch theorem due to W. Schmidt and a version of implicit function theorem due to M. Laurent and D. Roy. We denote by $H_K(\cdot)$ and $N_K(\cdot)$ the multiplicative height over K and the norm from K to $\mathbb{Q}$ respectively. Our main result is as follows:

Theorem 1 *Let $F(X,Y) = \sum_{i=0}^{m} \sum_{i=0}^{n} a_{ij} X^i Y^j$ be an absolutely irreducible polynomial in $O_K[X,Y]$, with $a_{00} = 0$ and $a_{01} \neq 0$. Let g be the genus of the curve $F(X,Y) = 0$. Set $N = max\{m, 2g+n+1\}$. If $\wp$ is a prime ideal of O_K with $N_K(\wp) \geq \Omega(F)$, where*

$$\Omega(F) = H_K(F)^{42N^7(d+1)} (N^{58} 2^{96N^2})^{N^5 d(d+1)},$$

then the reduction of $F(X,Y)$ modulo $\wp$ is an absolutely irreducible polynomial.

The case of an arbitrary absolutely irreducible polynomial in $O_K[X,Y]$ can be easily reduced in the case treated in Theorem 1. When the curve $F(X,Y) = 0$ is smooth, an elimination result of Lazard implies a better estimate for A.

Theorem 2 *Let $F(X,Y,Z) \in O_K[X,Y,Z]$ be an homogeneous absolutely irreducible polynomial of degree $N \geq 2$ such that the projective curve $F(X,Y,Z) = 0$ is smooth. Let Φ be a point with projective coordinates 1 and the coefficients of $F(X,Y,Z)$. If $\wp$ is a prime ideal of O_K with $N_K(\wp) \geq \Omega(F)$, where*

$$\Omega(F) = (N^{4d} H_K(\Phi))^{5N^2},$$

the reduction of $F(X,Y,Z)$ modulo $\wp$ is an absolutely irreducible polynomial.

QUER, JORDI
"*Fields of definition of $\mathbb{Q}$–curves*".

A $\mathbb{Q}$–curve is an elliptic curve $C/\overline{\mathbb{Q}}$ isogenous to all its Galois conjugates. We consider only $\mathbb{Q}$–curves with no complex multiplication. An abelian variety $A/\mathbb{Q}$ is of GL_2–type if the algebra $E = \mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}}(A)$ is a number field of degree $[E : \mathbb{Q}] = \dim A$.

In [1] Ribet characterizes $\mathbb{Q}$–curves as those elliptic curves that are quotients over $\overline{\mathbb{Q}}$ of an abelian variety of GL_2–type. In [2], he finds the smallest fields over which a $\mathbb{Q}$–curve can be defined, up to isogeny.

Let $C/\overline{\mathbb{Q}}$ be a $\mathbb{Q}$–curve. In this talk we characterize

(a) the fields $K/\mathbb{Q}$ such that there is a curve C' isogenous to C, defined over K and with the isogenies between Galois conjugates also defined over K,

(b) the pairs $(K, C'/K)$ as in (a) such that the abelian variety obtained by restriction of scalars $\mathrm{Res}_{K/\mathbb{Q}}(C'/K)$ is $\mathbb{Q}$–isogenous to a product of abelian varieties of GL_2–type.

Note that, assuming the Shimura–Taniyama conjecture: namely, that the abelian varieties of GL_2–type are precisely (up to isogeny) the varieties A_f attached by Shimura to newforms of weight two for $\Gamma_1(N)$, then the curves C/K' of part (b) are the elliptic curves over number fields whose L–series are products of L–series of cusp forms of weight two for $\Gamma_1(N)$.

References:

[1] K. Ribet, *Abelian varieties over $\mathbb{Q}$ and modular forms*, Proceedings of KAIST Mathematics Workshop (1992), 53–79.

[2] K. Ribet, *Fields of definition of abelian varieties with real multiplication*, Contemp. Math. 174 (1994), 107–118.

Raigorodskii, Andrei M.
"*A probabilistic approach to the problem of the defect of good admissible sets in a lattice*".

Let $\mathcal{E} = O, \mathbf{e}_1, \ldots, \mathbf{e}_n$ be the frame of unit coordinate vectors, let Λ be a lattice in $\mathbb{R}^n$ such that $\mathbb{Z}^n \subset \Lambda$, let $\{\Omega^n_{\mathcal{E}}\}_{n=1}^{\infty}$ be an arbitrary sequence of sets satisfying the following conditions: $\Omega^n_{\mathcal{E}} \subset [-1,1]^n \;\forall\, n \geq 1$, $\pm\mathcal{E} \subset \Omega^n_{\mathcal{E}} \;\forall\, n \geq 1$, and the section of $\Omega^n_{\mathcal{E}}$ by each k–dimensional coordinate subspace of $\mathbb{R}^n$ coincides with the set $\Omega^k_{\mathcal{E}}$ for all $1 \leq k \leq n$. A set $\Omega^n_{\mathcal{E}}$ is said to be *admissible in* Λ if $\Omega^n_{\mathcal{E}} \bigcap \Lambda = \{O, \mathbf{e}_1, \ldots, \mathbf{e}_n\}$. The *defect* $d(\Omega^n_{\mathcal{E}}; \Lambda)$, *with respect to* Λ, *of a set* $\Omega^n_{\mathcal{E}}$ *admissible in* Λ is the smallest number of vectors to be deleted from $\mathcal{E}$ in order that the remaining system can be complemented to a basis in Λ. Let $d_n(\Omega^n_{\mathcal{E}}) = max_{\Lambda}\, d(\Omega^n_{\mathcal{E}}; \Lambda)$ and let $d^*_n(\Omega^n_{\mathcal{E}}) = max^*_{\Lambda}\, d(\Omega^n_{\mathcal{E}}; \Lambda)$, where the maximum is taken over all Λ in the first case and over all Λ such that $\Lambda/\mathbb{Z}^n$ is a cyclic group in the second.

It follows from [1] and [2] that for the case, when $\Omega^n_{\mathcal{E}}$ is the unit octahedron, one can find estimates for $d^*_n(\Omega^n_{\mathcal{E}})$ sharp in order as $n \to \infty$. Moreover, it was shown in [3] how the methods proposed in [1] and [2] can be extended in order to find arguments for essentially more general class of results. The proofs presented in [1], [2] and [3] were based on some explicit combinatorial construction corresponding to the problem of determining the *minimal system of common representatives* (see [4] and [5] for details) and on methods of the geometry of numbers (see [6]). On the other hand, there exists another approach to the generalization of the results of the papers [1] and [2]. This approach involve the use of the probabilistic methods in combinatorics. In other words, the probabilistic method makes it possible to obtain independently some generalizations quite different from those described in [3]. The exact statements of all these results are rather cumbersome. So we do not formulate them in this abstract.

References:

[1] N.G. Moshchevitin, Mat. Zametki, V.58 (1995), p.558–568; English transl. in Math. Notes, V.58 (1995).

[2] A.M. Raigorodskii, Matematicheskii Sbornik, V.189, N6, p.117–141; English transl. in Sbornik: Mathematics, V.189, N6, p.931–954.

[3] A.M. Raigorodskii, Grazer Mathematische Berichte, 1999.

[4] N.N. Kuzyurin, Problemy Kibernet. 1980, N37, p.19–56 (Russian).

[5] A.M. Raigorodskii, Fundamentalnaya i Prikladnaya Matematika, 1999.

[6] P.M. Gruber, C.G. Lekkerkerker, "Geometry of numbers", North–Holland, Amsterdam 1987.

Rémond, Gaël
"*On the product theorem*".

The talk intends to present new sharp effective versions of Falting's product theorem. This result, a generalization of Roth's lemma, shows that if the zeroes of index σ of a multihomogeneous polynomial P have a component Z in common with the zeros of index $\sigma + \epsilon$ then this Z (subset of a product of projective spaces) is itself a product. Here the index is taken with respect to the degrees δ_i of P as weights and the result holds whenever δ_i/δ_{i+1} is big enough in terms of ϵ. Furthermore, effective versions by Evertse and Ferretti bound the degree and height of Z. If m is the number of factors and c the codimension of Z, our result assume only

$\delta_i/\delta_{i+1} \geq (m/\epsilon)^c$. This is better than the previous bounds by a factor $c!$ and we improve in the same way the estimates for degrees and heights. The key point is the use of Samuel multiplicity introduced in these questions by Philippon, through his zero-estimates. The main corollary of the theorem shows that, in the above setting, any component of the zeros of index ϵ are contained in a (non-trivial) product under a similar, more restrictive condition on the degrees of P. We deduce first such a corollary, in the usual manner, with the bound $\delta_i/\delta_{i+1} \geq (mn/\epsilon)^n$ (where n is the dimension of the multi–projective space). This condition is the one obtained by Philippon but we get slightly better estimates for degrees and heights (through a direct proof). Last, using a different approach, we prove another corollary with the better bound $\delta_i/\delta_{i+1} \geq (m/\epsilon)^n$; in this case estimates for degrees and heights are less accurate but not significantly in view of certain applications.

Roskam, Hans
"*Artin's conjecture on primitive roots over number fields*".

In 1927 Emil Artin made the following conjecture: for any integer α, the natural density

$$\lim_{x\to\infty} \frac{\#\{p \text{ prime} : p \leq x \text{ and } \langle\alpha\rangle = (\mathbb{Z}/p\mathbb{Z})^*\}}{\#\{p \text{ prime} : p \leq x\}}$$

of the set of primes p for which α is a primitive root modulo p inside the set of all prime numbers exists. This conjecture is still unproved, but in 1967 Hooley showed that it is a consequence of the generalized Riemann hypothesis.

We generalize Artin's conjecture as follows. Let K be a number field with ring of integers $\mathcal{O}$ and $\alpha \in \mathcal{O}$. For a rational prime p, the group $(\mathcal{O}/p\mathcal{O})^*$ is not in general cyclic; its structure depends on the splitting type of p in K. We say that the order of α in $(\mathcal{O}/p\mathcal{O})^*$ is *maximal* if it is equal to the exponent of $(\mathcal{O}/p\mathcal{O})^*$. Only if p is inert in K, the elements of maximal order are actually generators of $(\mathcal{O}/p\mathcal{O})^*$. Define the set S as

$$S = \{p \text{ prime} : \alpha \text{ has maximal order in } (\mathcal{O}/p\mathcal{O})^*\}.$$

In the talk we formulate a more precise version of the following theorem.

Theorem. *If K is quadratic and the generalized Riemann hypothesis holds, then S has a density inside the set of rational primes. Actually, both the set of primes in S that split in $K/\mathbb{Q}$ and the set of primes in S that are inert in $K/\mathbb{Q}$ have a density.*

In Artin's original conjecture, the density is zero if and only if α is a square or equal to -1. We will list all cases for which the density of S vanishes. As an example, we show that S has zero density for $\alpha = (\frac{15+3\sqrt{5}}{2})^{15}$.

Roy, Damien
"*On Schwarz lemma*".

The classical Schwarz lemma says that, if an entire function $f\colon \mathbb{C}^n \to \mathbb{C}$ vanishes to order $\geq n$ at the origin, then, for any reals r and R with $0 < r < R$, we have $|f|_r \leq \left(\frac{r}{R}\right)^n |f|_R$, where $|f|_\rho$ denotes the maximum of $|f(z_1,\ldots,z_n)|$ on the polydisk $\max\{|z_1|,\ldots,|z_n|\} \leq \rho$. For the purpose of transcendental number theory, it is useful to generalize this type of inequality for functions vanishing, with multiplicities, on more complicated subsets of $\mathbb{C}^n$. In this direction, Michel Waldschmidt proposed a conjecture concerning the growth of entire functions which vanish on large subsets of $\mathbb{C}^n$ consisting of linear combinations with bounded integral coefficients of a fixed set of vectors. In this talk, we describe the present state of this problem and and its connection with zero estimates. We prove a new Schwarz lemma and present an application of it to the exponential function.

RUDNICK, ZEÉV
"*Primitive roots and the quantized cat map*".

In the past few years, several interesting relations were discovered between Number Theory and the area of physics known as "Quantum Chaos". In this talk I discuss one such case: A relation between the classical Gauss–Artin problem on primitive roots and the problem of "quantum unique ergodicity" for the "quantized cat map".

The quantized cat map is a model system which starts with a hyperbolic matrix A in the modular group $SL(2,\mathbb{Z})$, and for each integer $N \geq 1$ associates to it a certain unitary $N \times N$ matrix $U_N(A)$, called the quantum propagator (the construction is a variant of the Weil representation). The problem is to understand certain properties of the eigenvectors of $U_N(A)$ as N tends to infinity. In doing this, one encounters issues concerned with the behavior of the order of the matrix A modulo N, related to the Gauss–Artin problem of showing that any integer (different from ± 1 or a perfect square) is a primitive root for infinitely many primes.

The talk will explain these concepts and is based on joint work with Par Kurlberg.

SHIGA, HIRINORI
"*Toward the quaternion $K3$ modular function*".

We study the period map for a family $\mathcal{F}$ of complex algebraic surfaces

$$V_x : z^2 = \prod_{i=1}^{4}(s_0, s_1)\begin{pmatrix} x_{11}^i & x_{12}^i \\ x_{21}^i & x_{22}^i \end{pmatrix}^t (t_0, t_1)$$

where $[s_0, s_1]$ and $[t_0, t_1]$ are homogeneous coordinates on $\mathbb{P}^1 \times \mathbb{P}^1$ and

$$x = (x^1, x^2, x^3, x^4) \in X = (GL(2,\mathbb{C}))^4 \quad \text{with} \quad x^i = \begin{pmatrix} x_{11}^i & x_{12}^i \\ x_{21}^i & x_{22}^i \end{pmatrix}$$

is a parameter.Generically V_x is a double covering over $\mathbb{P}^1 \times \mathbb{P}^1$ branched along different four type $(1,1)$ curves and it is a $K3$ surface.

Theorem 1 *Generically the transcendental lattice of V_x is of rank 8 and takes the form $T = U(2) \oplus U(2) \oplus (-2I_4)$. Conversely the $K3$ surface with this transcendental lattice is represented in the above form.*

Fact. We can construct the period map $\Phi : X^* \to \mathbb{P}^7$ and the period domain is described as

$$D = \{\eta = [\eta_1, \cdots, \eta_8] \in \mathbb{P}^7 : \eta A({}^t\eta) = 0, \overline{\eta} A({}^t\eta) > 0, \Im(\eta_3/\eta_1) > 0\}.$$

This domain has a modular embedding ρ into the Siegel upper half space $\mathcal{S}_8$. The embedded image is characterized as a Shimura variety induced from the extra endomorphism algebra $(-1,-1)_{\mathbb{Q}}$ (that is the Hamilton quaternion algebra over $\mathbb{Q}$).

Theorem 2 *Take an element $V_x \in \mathcal{F}$ and suppose the period $\eta \in \mathbb{P}^7$ is an algebraic point. Then V_x has an expression with algebraic parameter x if and only if $\rho(\eta)$ is a CM point.*

To obtain the last theorem we need the explicit construction of the Kuga-Satake variety corresponding to V_x.

Sodaigui, Bouchaib
"*Realizable classes of dihedral extensions of degree* 8".

We continue to study the set of Galois module classes of rings of integers in Galois extensions of algebraic number fields.

For every number field E, O_E denotes its ring of algebraic integers.

Let k be a number field and Γ a finite group. Let $\mathcal{M}$ be a maximal O_k–order in $k[\Gamma]$ containing $O_k[\Gamma]$ and $\mathcal{C}\ell(\mathcal{M})$ its class group. We denote by $\mathcal{R}(\mathcal{M})$ the set of realizable classes, that is the set of classes $c \in \mathcal{C}\ell(\mathcal{M})$ such that there exists a Galois extension N/k at most tamely ramified , with Galois group isomorphic to Γ and the class of $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$ in $\mathcal{C}\ell(\mathcal{M})$ is equal to c. It is known that $\mathcal{R}(\mathcal{M}) \subset \mathcal{C}\ell^{\circ}(\mathcal{M})$, where $\mathcal{C}\ell^{\circ}(\mathcal{M})$ is the kernel of the morphism $\mathcal{C}\ell(\mathcal{M}) \to \mathcal{C}\ell(k)$ induced by the augmentation $\mathcal{M} \to O_k$. When Γ is abelian, a consequence of the work of McCulloh (see L. R. McCulloh, Galois module structure of abelian extensions, J. Reine Angew. Math. 375/376, 1987, 259–306) is: $\mathcal{R}(\mathcal{M})$ is a subgroup of $\mathcal{C}\ell^{\circ}(\mathcal{M})$.

In this communication we study the problem of realizable classes when Γ is nonabelian in the case $\Gamma{=}D_4$ the dihedral group of order 8. We will prove the following result:

Theorem. *Suppose that the class number of k is odd, and that k is linearly disjoint from $\mathbb{Q}(i)$, where $i^2 = -1$. Then $\mathcal{R}(\mathcal{M})$ is the subgroup $\mathcal{C}\ell^{\circ}(\mathcal{M})$. In this case $\mathcal{C}\ell^{\circ}(\mathcal{M}) \cong \mathcal{C}l(k)^4$.*

Solé, Patrick
"*Ramanujan Geometries of type* $\widetilde{A}_n$".

(joint work with Don Cartwright (Sydney) and Andrzej Zuk (Lyon)).

A finite regular graph of degree k is said to be **Ramanujan** if the nontrivial part of its spectrum (the spectrum of its adjacency matrix) is contained (up to trivial $\pm k$ eigenvalues) not only in $[-k, k]$ as Perron-Frobenius would have it but in the smaller range $[-2\sqrt{k-1}, 2\sqrt{k-1}]$. The name of Ramanujan graph was introduced by Lubotzky, Phillips, Sarnak in relation with the Ramanujan conjecture on Fourier coefficients of cusp forms. The definition has been extended from regular graphs to bipartite graphs (Feng-Li), then to weighted graphs (Morgenstern), and, more recently, to multipartite graphs (Solé). In this work we give a definition of Ramanujanness which is adapted to graphs covered by the skeleton of an $\widetilde{A}_n$ building and we provide some theoretical and numerical evidence for the existence of such objects in the case of $n = 2$.

Sonn, Jack
"*Nilpotent Galois groups over* $\mathbb{Q}_{nil}(t)$".

Let $\mathbb{Q}_{nil}$ denote the maximal nilpotent extension of the rationals $\mathbb{Q}$. For every prime p, the free pro–p group on countably many generators is realizable as the Galois group of a (regular) extension of $\mathbb{Q}_{nil}(t)$. In particular, every finite nilpotent group is realizable as a regular extension of $\mathbb{Q}_{nil}(t)$. In an earlier paper of the author, this result was proved for the larger field $\mathbb{Q}_{abnil}$, the maximal nilpotent extension of the maximal abelian extension of $\mathbb{Q}$, using a local–global principle for embedding problems over rational function fields derived from the Faddeev–Auslander–Brumer theorem on the Brauer group of a rational function field, and applying the methods of Scholz–Reichardt–Shafarevich. The proof of the present result uses the same circle of ideas together with a classical descent argument.

Spriano, Luca
"*Ramification theory for complete discrete valuation fields*".

We study extensions L/K of complete discrete valuation fields K with residue field K of characteristic $p > 0$, which we do not assume to be perfect. Our work concerns ramification theory for such extensions, in particular we show that all classical properties which are true under the hypothesis *"the residue field extension*

L/K *is separable"* are still valid under the more general hypothesis that the valuation ring extension is monogenic. We also show that conversely, if classical ramification properties hold true for an extension L/K, then the extension of valuation rings is monogenic. These are the *"well ramified"* extensions. We show that there are only three possible types of well ramified extensions and we give examples. In the last part of the paper we consider, for the three types of well ramified extensions, Kato's generalization of the conductor, for which we exhibit an upper bound defined in terms of classical ramification invariants. For well ramified extensions we show the bound is sharp.

Stevenhagen, Peter
"*A two variable Artin conjecture*".

Artin's conjecture on primitive roots states that every non–square integer $a \neq -1$ is a primitive root modulo infinitely many primes p, and that the set of these p has a natural density $\delta(a)$. It was proved under GRH by Hooley in 1967.

Stephens showed in 1970 that the density $\delta(a, b)$ of the set of primes p for which b mod p is in the subgroup generated by a mod p can be determined in a similar way.

We present a corrected version of Stephens' result, and show how quadratic generalizations of the method can be used to attack the following problem posed by Lagarias in 1985 in the paper 'The set of primes dividing the Lucas numbers has density 2/3': determine the density of the set of primes dividing some term of the integer sequence $\{x_n\}_{n\geq 0}^{\infty}$ defined by $x_0 = 3$, $x_1 = 1$ and $x_{n+1} = x_n + x_{n-1}$ for $n \geq 1$.

This is joint work with Pieter Moree.

Ramana, D. Surya
"*Atkin's Theorem on Psuedo–squares*".

A.O.L. Atkin [Proc. London Math. Soc. (3) 14, 22-27(1965)] proved the existence of an infinite sequence of natural numbers, whose j–th term $s(j)$ satisfies $s(j) = j^2 + O(\log j)$, such that the set of integers representable as a sum of two distinct elements of this sequence has positive asymptotic density.

Atkin's proof involves the estimation of a certain integral using the circle method. I shall present an elementary proof of this result.

The contents of my proposed talk have appeared as R.Balasubramanian and D.S.Ramana, Atkin's Theorem on Psuedo–squares, Publ. Inst. Math. (Beograd), 63(77), 21–25, 1998.

Swallow, John R.
"*Explicit Quadratic Descent for Quaternion Algebras*".

Let L/K be a quadratic extension of fields of characteristic not 2, and $A = (a, b)_L$ be a quaternion algebra over L. A theorem of Arason establishes that A *descends* to K, i.e., $[A] = [(c, d)_K \otimes_K L] \in \mathrm{Br}_2(L)$, iff $[\mathrm{cor}_{L/K} A] = 1 \in \mathrm{Br}_2(K)$, where Br_2 denotes the 2-torsion in the Brauer group and cor is algebra corestriction. Using the theory of Galois embedding problems with kernel $\mathbb{Z}/2\mathbb{Z}$, we derive explicit formulas for c and d in terms of a, b, and f, where f is an explicit isomorphism $f : \mathrm{cor}_{L/K} A \cong Mat_{4\times 4}(K)$. Combining this result with the fact that the corestriction may be calculated explicitly in terms of a and b, we explicitly reduce the determination of the triviality of $[A] \in \mathrm{Br}_2(L)$ to the question of whether $[(c, d)] \in \mathrm{Br}_2(L/K)$. We discuss applications to the calculation of obstructions to Galois embedding problems with kernel $\mathbb{Z}/2\mathbb{Z}$, particularly over number fields.

RAVINDRANATHAN, THANGADURAI
"*On a Lattice Point Problem*".

We prove if for every $n \geq 3$, we are given a sequence of $4n-3$ number of integer lattice points in the plane such that one of the lattice points is repeated at least $[n/2]$ times, then we can find an n element subsequence whose sum is zero modulo n in both the co ordinates. When n is even, one obtains a little better result. More precisely, if we assume that one of the lattice points is at least $n/2-1$ times repeated, then the result is true.

Let $f(n,2)$ be the smallest positive integer such that any given $f(n,2)$ number of integer lattice points in the plane, we have an n subsequence whose sum is zero modulo n in both the co ordinates. We prove that if $f(n,2)=4n-3$ and $n>(3m^2-m+3)/4, m \geq 2$, then $f(nm,2)=4nm-3$. Both these results improve the results of W. Gao.

We start our talk with a description of the history of the problem and then the sketch of the proofs of our results.

TERAI, NOBUHIRO
"*The Diophantine equation* $a^x - b^y = d$".

Let $a,\ b,\ d$ be positive integers with $a \geq 2$ and $b \geq 2$. Pillai [4] showed that the Diophantine equation

$$a^x - b^y = d \tag{1}$$

has only finitely many positive integral solutions x, y. Pillai [5] also showed that when d is sufficiently great with respect to a and b, equation (1) has at most one solution x, y.

In this talk, using a lower bound for linear forms in two logarithms due to Mignotte [2], we give the effective upper bound of the solution y of equation (1) in terms of a under a certain condition. Applying this upper bound and the continued fraction expansion of $\dfrac{\log b}{\log a}$, we can solve equation (1) completely when d is relatively "small". The methods for solving equation (1) so far were elementary or algebraic method using the congruent, quadratic fields and cubic fields etc.. We give some examples, e.g., the equation $2^x - 3^y = 5$. (cf. Nagell [3], Herschfeld [1].)

References:

[1] A. Herschfeld, *The equation* $2^x - 3^y = d$, Bull Amer. Math. Soc. 42(1936), 231–234.

[2] M. Mignotte, *A corollary to a theorem of Laurent–Mignotte–Nesterenko*, Acta Arith. **86** (1998), 101–111.

[3] T. Nagell, *Sur une classe d'équations exponentielles*, Ark. Mat. **3** (1958), 569–582.

[4] S.S. Pillai, *On the inequality* $0 < a^x - b^y \leq n$, J. Indian Math. Soc. **19** (1931), 1–11.

[5] S.S. Pillai, *On* $a^x - b^y = c$, J. Indian Math. Soc. (New Series), **2** (1936), 119–122, Corr. **2** (1936), 215.

THUSWALDNER, JÖRG M.
"*The sum of digits function for number system with negative bases*".

Let $q \geq 2$ be an integer. Then $-q$ gives rise to a number system in $\mathbb{Z}$, i.e. each number $n \in \mathbb{Z}$ admits a unique representation of the form

$$n = c_0 + c_1(-q) + \cdots + c_h(-q)^h$$

with $c_j \in \{0, 1, \ldots, q-1\}$. In my lecture I present some results on the sum of digits function ν_{-q} of these number systems. In particular, I discuss the asymptotics of its summatory function and the asymptotics of

$$\sum_{n<N} |\nu_{-q}(n) - \nu_{-q}(-n)|.$$

For this sum one can obtain an asymptotic distribution result. I will show the methods used in the proofs of these results. There were used automata as well as analytical methods.

Thiebaud, Caroline
"*Capitulation dans un corps des genres*".

Dans cet expose, on aimerait generaliser au corps des genres d'une extension abelienne d'un corps de nombres le theoreme de l'ideal principal: "Tout idéal de k est principal dans son corps de Hilbert". Ainsi, on s'interesse a la capitulation des classes d'ideaux ambiges dans le corps des genres d'une extension abelienne d'un corps de nombres. En fait on souhaite etendre a un corps de base quadratique imaginaire un resultat de Hisako Furuya qui traite le probleme lorsque le corps de base est le corps des rationnels. En effet, on peut encore dans ce cas donner une construction explicite des corps de rayon a l'aide de la theorie de la multiplication complexe et fournir des generateurs explicites pour les ideaux.

Ullmo, Emmanuel
"*Distribution of algebraic points*".

Vela, Montse
"*Embedding problems with cyclic kernel*".

We study embedding problems given by a central extension with kernel $\mathbb{Z}/n\mathbb{Z}$ $(2 \leq n \in \mathbb{Z})$ over a field K with $carK \nmid n$ and $\mu_n \subset K$ ($\mu_n =$ group of n–th roots of unity). Our main achievements are an expression for the obstruction to the solvability of these embedding problems in terms of easily computable Galois symbols and a method to construct the solutions when the problems are solvable.

First, we study continuous representations of a profinite group in the graded automorphism group of a generalized Clifford algebra. We define some cohomology classes associated to the representation and the modified algebra. We obtain a formula that connects Brauer invariants of the algebra and the modified algebra with the defined cohomology classes.

Then, we compute the obstruction to the solvability of embedding problems given by exact sequences $0 \to \mathbb{Z}/n\mathbb{Z} \to E \to \mathbb{Z}/n\mathbb{Z} \times \cdots \times \mathbb{Z}/n\mathbb{Z} \to 0$. Finding adequate representations for each example, we express the obstruction as a sum of Galois symbols.

Finally, we give a method to construct the solutions to solvable embedding problems with kernel $\mathbb{Z}/n\mathbb{Z}$. We use this method to compute the explicit solutions for problems given by the exact sequences

$$1 \to \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n^2\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 1 \text{ and } 1 \to \mathbb{Z}/n\mathbb{Z} \to E \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to 1.$$

We develop the package **n–Clifford**, a set of programs in *Mathematica* designed to performs explicit calculations on $K(\sqrt[n]{a})$ and on generalized Clifford algebras. This package allows calculations for any n.

Voskresenskaya, Galina
"*Metacyclic groups and multiplicative η–functions*".

In the previous works of the author it was proved that there are
only 28 functions determined by the following conditions:
these functions are
1) cusp functions of integral weight with characters;
2) eigenforms of the Hecke algebra;
3) they have no zeroes outside of the cusps.
They can be described completely by the following formulas:

$$f(z)=\prod_{k=1}^{s}\eta^{t_k}(a_k z),\quad a_k,\ t_k\in\mathbb{N},\sum_{k=1}^{s}t_k a_k=24,$$

$$2|\sum_{k_1}^{s}t_k,\ a_k|a_s,\ a_1a_s=a_{s+1-k}a_k, 1\le k\le s,$$

where $\eta(z)$ is Dedekind's η–function.
We add to this list two modular forms of half–integral weight: $\eta(24z),\eta^3(8z)$.
All this functions we shall call *multiplicative η–functions*
because of their multiplicative Fourier coefficients.

Theorem. *Let G be a metacyclic group:*

$$\langle a,b: a^m=e,\ b^s=e,\ b^{-1}ab=a^r\rangle,$$

such that there is an exact representation T that for every $g\in G$ the characteristic polynomial of the operator T(g) has such form

$$\prod_{k=1}^{s}(x^{a_k}-1)^{t_k},$$

that the corresponding cusp form

$$\eta_g(z)=\prod_{k=1}^{s}\eta^{t_k}(a_k z)$$

is multiplicative η–product.

Then if $m=3,4,5$ than for s and r there are only the following possibilities:
$m=3,\ r=2, s=2,4,6,8,12,18;$
$m=4,\ r=3, s=2,4,6,8,10,24;$
$m=5,\ r=2, s=4,8,12;$
$m=5, r=4, s=2,4,6,8.$

Walling, Lynne
"*Siegel modular forms, Hecke operators and theta series*".

We use the language of lattices to succinctly describe the action of the Hecke operators on the Fourier coefficients of Siegel modular forms. We also describe the action of the Hecke operators on theta series.

Wallisser, Rolf
"*A theorem on entire functions as a principle for proof's on irrationality*".

Using ideas of D. Bertrand and G. Chudnovsky the following can be proved:

Theorem. *Let f be an entire transcendental function taking with all its derivatives rational values at the points w_1 and w_2 of a quadratic number field. If the order of f is smaller than two and if there is a constant C such that the least common multiple of the denominators $q_1,\dots,q_k$ of the values $f^{(\nu)}(w_i)$, $0\le\nu\le k$, $i=1,2$ is smaller than C^k, then the points w_1 and w_2 have to be equal.*

From this nearly all known results on irrationality at rational points for elementary functions can be derived. A slight generalization of the theorem can be applied to give results on irrationality for values of functions like the incomplete Gamma function or to show the irrationality of certain irregular continued fractions.

Wewers, Stefan
"*Cohomological obstruction for the field of definition of Galois covers*".

Let G be a finite group and $\varphi : X \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ a G–Galois cover of the projective line over $\bar{\mathbb{Q}}$. By a result of Fried and Völklein, φ corresponds to a $\bar{\mathbb{Q}}$–rational point $[\varphi]$ of a Hurwitz space $H_r(G)$. Let K be the *field of moduli* of φ, i.e. the field of rationality of the point $[\varphi]$. Then φ can be defined over K if and only if a certain obstruction

$$\omega_\varphi \in H^2(K, Z_G)$$

vanishes (here Z_G is the center of G). By a result of Dèbes/Douai/Emsalem, the obstruction ω_φ is the specialization of a global obstruction

$$\tilde{\omega} \in H^2(H_r(G), Z_G)$$

on the Hurwitz space. In this talk we describe how one can obtain information on ω_φ and $\tilde{\omega}$ by extending $\tilde{\omega}$ to a compactification $\bar{H}_r(G)$ of the Hurwitz space à la Harris/Mumford. We will give some examples and discuss applications to the Regular Inverse Galois Problem.

Winterhof, Arne
"*Results on Waring's problem in finite fields*".

Let $g(k, p^n)$ be the smallest s such that every element of the finite field $\mathbb{F}_{p^n}$ is a sum of s kth powers in $\mathbb{F}_{p^n}$. We summarize known estimates of $g(k, p^n)$ and prove for $n \geq 2$

$$\max_p\{g(k,p^n) | \frac{p^n-1}{p^d-1} \not| k \forall d | n, d \neq n\} < 6.1 n k^{2/n}.$$

Wolf, Marek
"*The computer search for primes of the form* n^2+1".

The results of the over two CPU years computer hunt for the primes of the form $n^2 + 1 = 4k^2 + 1$ up to 2×10^{16} are reported. By E conjecture of Hardy and Littlewood the number $\pi_{x^2+1}(n)$ of primes of this form smaller than n should be asymptotically $\int_2^n \frac{du}{\sqrt{u}\log(u)}$. The number of sign changes of the difference $\pi_{x^2+1}(n) - \int_2^n du\sqrt{u}\log(u)$ and the error term is investigated. The distribution of values of the k factors of $n = 2k$ display unexpected regularities and the conjecture about differences between two consecutive $k's$ giving $4k^2 + 1$ prime is formulated. The formula describing behaviour of the gaps between primes of the form $n^2 + 1$ is also conjectured. The primes of the form $n^2 + 1$ are congruent to 1 or 7 modulo 10 and heuristic arguments give that those congruent to 7 should be two times more than these congruent to 1, what agrees quite well with the computer results. Also the primes of the form $4p^2 + 1$, where p is a prime, are investigated.

Wooley, Trevor
"*Exponential sums and diophantine problems: the unexpected afterlife of classical ideas*".

Classical approaches to problems in additive number theory seem to have been trampled to death by the continuing advances of the Hardy-Littlewood method and the theory of exponential sums. Recently, however, progress has stemmed from innovations with a surprisingly classical flavour, and these ideas have spawned progress in our understanding of the theory of Waring's problem, and more general diophantine problems. In this talk we will survey as many of these developments as time permits, discussing in particular the solubility of additive diophantine equations and Waring's problem, but also pointing to developments more general in their application.

Yanchevskii, Vyacheslav I.
"P–primary torsion of Brauer groups of local elliptic curves with bad reduction and unramified division algebras over their function fields".

Let k be a local field of zero characteristic, E an elliptic curve over k and $Br\ E$ its Brauer group. It is known that $Br\ E$ is isomorphic to the unramified Brauer groups of function field $k(E)/k$ ([1]). Any element of the last group comes from a corresponding unramified central division algebra over $k(E)$. So far it is almost nothing known about such algebras. Some time ago (cf [2]) unramified division algebras of 2–primary indices (over k(E)), were described. The purpose of the talk is to present similar results in case where E has bad reduction and unramified division algebras are of p–primary indices (where p is an arbitrary prime number). We use Tate p–adic uniformization in case of split multiplicative reduction (cf[3],[4]) and suggest an algorithm for translation of the form of generators of unramified division algebras expressed in terms of Wierstrass products to the usual language of elliptic functions. In general case of bad reduction our results combined with results of [2] give a complete description of such algebras.

Semilas results for curves over fields of formal power series $\mathbb{C}\langle t\rangle$ and $\mathbb{R}\langle t\rangle$ will be also presented.

References:

[1] Colliot–Thélène J.–P.(with the collaboration of J.–J. Sansuc). The rationality problem for fields of invariants under linear algebraic groups (with special regard to the Brauer group). Unpublished Lecture Notes from the 9th ELAM, Santiago de Chile, 1988.

[2] Yanchevskii V.I. Two–primary torsion of Brauer groups of local elliptic curves and unramified division algebras over their function fields. Journées Arithmétiques. Abstracts of talks, Barseona, July 16–20, 1995

[3] Silverman J.H. Advanced topics in the arithmetic of elliptic curves. Springer–Verlag, 1985

[4] Roquette P. Analytic theory of elliptic curves over local fields. Vandenhoeck & Ruprecht, Göttingen, 1970.

Yato, Mitsuaki
"On the extensions of the group schemes $\mathcal{G}^{(\lambda)}$ by $\mathbb{G}_a$ over a $\mathbb{Z}_{(p)}$–algebra".

Throughout this talk, p denotes a prime number, A a $\mathbb{Z}_{(p)}$–algebra, and λ an element in A. Let $\mathbb{G}_{a,A} :=$ Spec $A[T]$ denote the additive group scheme over A and $\mathcal{G}^{(\lambda)} :=$ Spec $A[T, \frac{1}{1+\lambda T}]$ the group scheme over A with the law of multiplication $T \mapsto \lambda T \otimes T + T \otimes 1 + 1 \otimes T$. We assume that $\mathcal{G}^{(\lambda)}$ acts on $\mathbb{G}_{a,A}$ trivially. $\mathrm{Ext}^1_A\left(\mathcal{G}^{(\lambda)}, \mathbb{G}_{a,A}\right)$ denotes the group formed by the classes of extensions of $\mathcal{G}^{(\lambda)}$ by $\mathbb{G}_{a,A}$.

Weisfeiler [3] gave an explicit description of the group $\mathrm{Ext}^1_A\left(\mathcal{G}^{(\lambda)}, \mathbb{G}_{a,A}\right)$, when A is an integral domain containing a field. Sekiguchi–Suwa [2] worked when A is a discrete valuation ring. Our aim of this talk is to generalize the result for any $\mathbb{Z}_{(p)}$–algebra A and also describe the group $\mathrm{Hom}\left(\mathcal{G}^{(\lambda)}, \mathbb{G}_{a,A}\right)$.

Definition. We define an endomorphism of $A^{(\mathbb{N})}$ denoted Φ by

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \end{pmatrix} \longmapsto \begin{pmatrix} -(-\lambda)^{p-1} & p & & \mathbf{0} \\ & -(-\lambda)^{p^2-p} & p & \\ \mathbf{0} & & \ddots & \ddots \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \end{pmatrix}.$$

Definition. We define polynomials $F_i(\Lambda; X, Y)$ in $\mathbb{Z}_{(p)}[\Lambda; X, Y]$ by

$$F_i(\Lambda; X, Y) = -\frac{1}{(-\Lambda)^{p^i-1}}(\partial^1 L_{i-1}(\Lambda; T))(X, Y)$$

for all $i \geq 1$, where

$$L_e(\Lambda; T) := p^e \sum_{i=1}^{p^{e+1}-1} \frac{(-\Lambda)^{i-1}}{i} T^i \in \mathbb{Z}_{(p)}[\Lambda; T]$$

for all $e \geq 0$, and

$$(\partial^1 L_e(\Lambda; T))(X, Y) := L_e(\Lambda; X) + L_e(\Lambda; Y) - L_e(\Lambda; \Lambda XY + X + Y).$$

Under the above definitions, our result is stated precisely as follows:

Theorem 1 *The correspondence*

$$(a_r)_{r\geq 0} \mapsto f(T) = \sum_{r\geq 0} a_r \left[\sum_{i=p^r}^{p^{r+1}-1} \frac{p^r}{i} (-\lambda)^{i-p^r} T^i \right]$$

induces an isomorphism $\operatorname{Ker} \Phi \xrightarrow{\sim} \operatorname{Hom}\left(\mathcal{G}^{(\lambda)}, \mathbb{G}_{a,A}\right)$.

Theorem 2 *The correspondence*

$$(b_i)_{i\geq 0} \mapsto g(X, Y) = \sum_{i\geq 0} b_i F_{i+1}(\lambda; X, Y)$$

induces an isomorphism $\operatorname{Coker} \Phi \xrightarrow{\sim} H_0^2\left(\mathcal{G}^{(\lambda)}, \mathbb{G}_{a,A}\right) \simeq \operatorname{Ext}_A^1\left(\mathcal{G}^{(\lambda)}, \mathbb{G}_{a,A}\right)$.

References:

[1] M.Lazard, *Sur les groupes de Lie formels à un paramétre*, Bulletin de la Societe Mathematique de France **83** (1955), pp.251–274.

[2] T.Sekiguchi, N.Suwa, *Some cases of extensions of group schemes over a discrete valuation ring I*, Journal of The Faculty of Science, the University of Tokyo, Sec.IA, Vol. **38**, No.1, pp.1–45.

[3] B.Weisfeiler, *On a case of extensions of group schemes*, Transactions of the American Mathematical Society, Vol.248, No. **1** (1979), pp.171–189.

Zaccagnini, Alessandro
"*Conditional density theorems for the zeros of the Riemann zeta–function*".

We find zero–free regions and density theorems for the Riemann zeta–function depending on non–trivial estimates for

$$J(x, \theta) := \int_x^{2x} |\psi(t) - \psi(t - \theta t) - \theta t|^2 dt,$$

uniformly in some range of θ. In a sense, this gives a sort of converse to the well–known results which relate zero–density estimates with good bounds for J. The general philosophy is that good estimates for J yield good zero–free regions for the zeta–function, provided that the range of uniformity for θ is large enough.

The proof is achieved by means of a suitable modification of the proof of a Density Theorem due to Bombieri (see Théorème 14 of [1]), using the Second Main Theorem of Turán. The fact that the zeta–function is of finite order in the critical strip also plays a crucial rôle.

References:

[1] E. Bombieri, *Le Grand Crible dans la Théorie Analytique des Nombres*, Astérisque n. 18 Societé Mathématique de France Paris 1974.

[2] *A conditional density theorem for the zeros of the Riemann zeta–function* (1999) Submitted for publication.

Zhan, Tao
"*Additive problems involving prime squares*".

In this talk some additive problems involving prime squares are discussed. For instance, it was proved jointly by J.Y. Liu, M.C. Liu and myself that every large even integer can be represented as sum of four prime squares and a bounded number of powers of 2, which gives a generalization of the well- known result of Linnik–every large odd integer is sum of two primes and a bounded number of powers of 2. We can now further show that the density of even integers representable as sum of two prime squares and k powers of 2 amony all even integers tends to 1 as k tends to infinity. Some other results concerning additive problems involving prime squares are also given in this talk.