Diophantine methods, lattices, and arithmetic theory of quadratic forms

Wai Kiu Chan (Wesleyan University),
Lenny Fukshansky (Claremont McKenna College),
Rainer Schulze-Pillot (Universität des Saarlandes, Saarbrücken),
Jeff Vaaler (University of Texas, Austin)

November 13 – 18, 2011

1 Overview of the Field and Recent Developments

The study of equations over the integers or the rational numbers is the subject of diophantine geometry. This also includes generalizations to finite extensions of the rationals, their rings of integers, and also to function fields over a finite field, and the rings of polynomials therein. This is a vast subject, in which a variety of methods from geometry, analysis, and arithmetic are used. For our intended workshop we focus on problems involving height functions, methods from the geometry of numbers, and the arithmetic of lattices with quadratic and hermitian forms. In the sections to follow we present a brief overview of a few directions in the theories of *height functions* and of *quadratic forms*, in particular concentrating on the interplay of these two lively areas.

1.1 Height functions and Diophantine problems.

Height functions of various sorts have played a fundamental role in diophantine problems. Height functions are used to measure the complexity of an algebraic object such as a polynomial or a point on an algebraic variety. A comprehensive account of their role in the modern theory of diophantine equations is contained in the recent monograph "Heights in diophantine geometry" by E. Bombieri and W. Gubler. In addition to this, a new research direction has been stimulated by recent work of Allcock and Vaaler on the metric space structure induced by certain height functions. If $h(\alpha)$ denotes the absolute Weil height on the nonzero algebraic number α, then $h(\alpha) = h(\zeta\alpha)$ for all roots of unity ζ. It follows that the height h is well defined on the quotient group $\overline{\mathbb{Q}}^{\times} / \operatorname{Tor}\{\overline{\mathbb{Q}}^{\times}\}$, where $\overline{\mathbb{Q}}^{\times}$ denotes the multiplicative group of nonzero algebraic numbers, and $\operatorname{Tor}\{\overline{\mathbb{Q}}^{\times}\}$ is its torsion subgroup. In fact $\overline{\mathbb{Q}}^{\times} / \operatorname{Tor}\{\overline{\mathbb{Q}}^{\times}\}$ has the structure of a vector space over $\mathbb{Q}$ (written multiplicatively), and h is a norm on this vector space. It follows that the metric completion is a Banach space over the real numbers. This Banach space has recently been investigated and shown to be isometric to a co-dimension one subspace of L^1 of a certain explicitly given measure space. Moreover, the measure that naturally arises is the unique invariant measure with respect to the action of the absolute Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$. Hence this group acts as a group of isometries on the Banach space. One expects that a similar but more elaborate structure will hold for the metric completion of elliptic curves, or more generally for abelian varieties, with respect to suitable height functions.

An important application of height functions to the study of diophantine equations arises from Northcott's finiteness property: there are only finitely many projective points over an algebraic number field with height bounded from above by a given constant. Hence, if one can prove that a given diophantine equation has a non-trivial solution of explicitly bounded height, then finding such a solution is reduced to a finite search. Therefore such bounds on heights are often referred to as *search bounds* for solutions of diophantine equations. This idea is frequently used in diophantine geometry when looking for points on varieties over number fields. In fact, in recent years there have been a number of results by a variety of authors on counting the number of points of bounded height on varieties, in particular in the direction of influential conjectures of R. Heath-Brown and Y. Manin.

On the other hand, one cannot expect the existence of explicit search bounds for diophantine equations of arbitrary degree in an arbitrary number of variables: This would provide an algorithm for deciding whether an equation has a solution, thus contradicting Matiyasevich's famous undecidability result for Hilbert's tenth problem. The only hope to obtain such search bounds for equations in a large number of variables is by restricting the degree, and it is known that even for a single equation of degree four search bounds already cannot exist. The two extensively studied situations here are that of a system of linear equations and of one quadratic equation. The first of these is addressed by Siegel's lemma and its many different generalizations, while the second stems from the work of J. W. S. Cassels on small-height zeros of quadratic forms. Cassels' theorem, proved in 1955, states that any isotropic rational quadratic form has a non-trivial rational zero of small height, where the explicit bound on height depends on the height of the coefficient vector of the form and its number of variables. There has been a large amount of work done by many authors ever since 1955 on various generalizations and extensions of Cassels' theorem. The investigation of height bounds for zeros of quadratic, hermitian, and bilinear forms, as well as the effective structure of corresponding bilinear spaces, not only carries independent number theoretic interest, but also contributes to our understanding of the boundary of Diophantine undecidability.

Another active direction of research closely connected to the above discussion is the study of classical and generalized Hermite constants, as well as related extensions of the classical geometry of numbers. Hermite's constant for a lattice Λ in $\mathbb{R}^N$ is defined to be

$$\gamma(\Lambda) = \frac{\min_{\boldsymbol{x} \in \Lambda \setminus \{\boldsymbol{0}\}} \|\boldsymbol{x}\|^2}{\det(\Lambda)^{1/N}} = \frac{\min_{\boldsymbol{y} \in \mathbb{Z}^N \setminus \{\boldsymbol{0}\}} Q_\Lambda(\boldsymbol{y})}{\det(Q_\Lambda)^{1/2N}},$$

where Q_Λ is a positive definite quadratic form on Λ. Hermite's constant is fundamental in lattice theory and discrete optimization problems, in particular in connection with sphere packing. In recent years new generalizations of the classical Hermite constant using height functions have been defined in adele spaces and algebraic groups over number fields. Hermite's constant in the non-commutative setting of central simple algebras has also been investigated, for instance in the works of J. Thunder and T. Watanabe. The study of generalized Hermite constants is a promising new direction, emphasizing the interplay of the arithmetic theory of quadratic forms with the theory of height functions.

1.2 Quadratic forms.

The arithmetic theory of quadratic (and hermitian) forms is on the one hand a subfield of the theory of diophantine equations, dealing with a particularly simple class of equations whose zero sets are also simple from the point of view of algebraic geometry. It has special features since the orthogonal group of a rational quadratic form provides a large group of automorphims which allows to bring group theoretic, representation theoretic, and ergodic methods into play. A recent spectacular success of these methods is the theorem of Ellenberg and Venkatesh on representation of quadratic forms by quadratic forms. A more classical but still very active group theoretic aspect (the oscillator representation and the theta correspondence) is at the basis of the use of the theory of modular forms for the investigation of quadratic forms, yet another group theoretic connection is the construction of lattices (or equivalently integral quadratic forms) using the theory of finite groups, as shown for example in Griess' recent work on the Barnes-Wall lattice. These aspects give the arithmetic theory of quadratic forms a special status in the larger field of diophantine equations.

The subject has seen dramatic progress in the twentieth century through the work of Siegel, Witt, Eichler, Kneser, Tamagawa, and it continues to flourish. The local-global principle for rational quadratic forms together with the strong approximation theorem for the spin group allows to reduce many (though by no means all) questions about integral quadratic forms to computations over the integers of a local field. Most of these local problems have been well understood in the case of odd residue characteristic for quite some time; the case of residue characteristic 2 (the dyadic case) presents, especially if 2 is ramified, considerable technical and conceptional difficulties. Remarkable progress has been obtained here by Nicu Beli in 2004, completing the determination of the spinor norm groups of lattices over the integers of general dyadic local field and of similar local groups arising in connection with the representation problem.

The global representation problem of integral quadratic forms is dealt with by a variety of methods, some of which have already been mentioned above. In 2009 Colliot-Thélène and Xu Fei showed that some of the difficulties arising here can be interpreted as an analogue of the well known Brauer-Manin obstruction in arithmetic geometry. Brüdern, Fouvry, Greaves, Heath-Brown, Blomer and Dietmann used new refinements of the classical Hardy-Littlewood circle method in conjunction with other arithmetic methods to prove results about representation of integers as sums of squares with restricted variables. Remarkably, classical analytic techniques, such as Hardy-Littlewood circle method, were also successfully used by Heath-Brown, Dietmann, Browning, and others to obtain new height search bounds for diophantine equations extending the classical results of Cassels and Siegel and their generalizations, as well as in the direction of Manin's conjecture. Hence investigations in the theory of heights frequently appeal to techniques quite similar to those commonly used in the arithmetic theory of quadratic forms. Moreover, many problems of diophantine geometry involve at some point arguments from the classical geometry of numbers and from the study of the arithmetic of particular definite or indefinite rational or integral quadratic forms, e. g. in the study of the Néron-Tate height on abelian varieties. More recently, in 1990s and 2000s, such classical ideas and techniques played an important role in the development of the deep and influential general theory of heights as seen in the works of: J.-B. Bost, H. Gillet, and C. Soulé; S. Zhang; S. David and P. Philippon; M. Sombra; E. Bombieri, D. Masser, and U. Zannier, and many others. A combination of theoretically obtained bounds for the size or number of solutions or for existence of representations for sufficiently large integers or forms and a computer assisted search below those bounds have in several cases proven to be extremely successful, for example in forthcoming work of Bhargava and Hanke on the 290-conjecture of Conway and in work of Jenkins and Rouse on the computation of minima of high-dimensional lattices.

Important progress has also been obtained recently in the area of reduction theory and construction of lattices with special properties (e. g. large minimum, specified automorphism group), where again often combinations of theoretical and computer assisted methods are successful. As examples we mention work of Schürmann, Watanabe, Gunnells, Yasaki on perfect forms and on Voronoi reduction and the construction of an extremal lattice in dimension 72 by Nebe.

2 Outcome of the Meeting and Scientific Progress Made

The goal of this workshop was to bring together people working in the following areas:

1. Classical arithmetic theory of quadratic forms and lattices.
2. Diophantine problems and the theory of height functions.

In spite of the close connections between these areas, it is quite rare for mathematicians working in these subjects to meet altogether for a joint workshop. Our workshop provided such a unique opportunity, which has certainly resulted in fruitful mathematical communication and will hopefully lead to significant future progress. There is a variety of prominent research directions that lie in the intersection of these two areas. Here are just a few of them:

1. Representation problems for quadratic forms and lattices over global fields and rings; finding representatives of small height in orbits of representation under the automorphism group of the form and counting representations of bounded height.
2. Small zeros (with respect to height) of individual quadratic forms and of systems of quadratic forms, originating in the work of Cassels and Siegel, its various generalizations, and related Diophantine problems with the use of heights.
3. Classical Hermite constant, geometry of numbers, and various generalizations with the use of height functions, explicit reduction theory of definite and indefinite quadratic forms.

Diophantine methods with the use of height functions are usually based on geometry of numbers and ideas from lattice theory. The target of these methods often lies in the realm of quadratic forms theory.

A proceedings volume of our workshop will be published in the AMS Contemporary Mathematics series. We feel that we met our goals of bringing together two mathematical communities and helping to start some new research directions. We include below comments from a few of our participants about the usefulness of the workshop from their perspective.

From Tim Browning (University of Bristol):

Of all the lectures at the conference I found the one by Colliot-Thelene the most inspiring. It deals with a problem that is right at the limit of what analytic number theory can handle and I plan to look at papers of Hooley from 2006 to see whether one can use the circle method to handle strong approximation for q(x,y,z)=P(t) when q is positive definite. The meeting was also very useful in that it gave me the opportunity to talk to Colliot-Thelene about the "state of affairs" for conic bundle surfaces with many split degenerate fibers, which has given me very useful motivation about a problem that I've recently started looking at (from the point of view of additive combinatorics) with a student of Ben Green (Lilian Matthiesen a postdoc at Bristol). Generally I greatly enjoyed meeting people that I don't normally encounter on the conference circuit and some of interactions led to useful and quite unexpected conversations about different aspects of quadratic forms and Thue type inequalities.

From Juan Marcos Cervino (University of Heidelberg):

Besides the fact, that being invited to a Workshop at BIRS is already a great pleasure (as one speaker mentioned: is one of the things a mathematician should do, as in normal life one should plant a tree..), I am very glad having had the opportunity to attend it. I would like to summarize my experience in the following items.

- It is always a pleasure to be in a place, where one feels oneself welcomed. This is the case for the whole BIRS (installations, personnel, et cetera). This being naturally the basis of a pleasant stay of any kind, which in our particular case certainly contributed to the effectiveness of the Workshop.

- The not so compressed schedule enabled us, the participants, to speak about our research interests in a less rigid atmosphere than within the talks themselves (the given schedule being certainly the "golden ratio", since on the other hand I would have liked to give a talk, as certainly others). For example, I got to know Prof. R. Coulangeon, who got interested in part of my research and is going to invite me to Bordeaux (France) to talk more precisely about the relations between his and my work. I discussed also with Prof. G. Nebe on a problem which was already pointed out to me by Prof. B. Venkov some weeks ago in Aachen. We will pursue this investigation further.

- Specialized Conferences or Workshops help younger mathematicians, I mean 'not so experienced mathematicians' (as is my case), to extract the main problems in the area, which may orient ideas and research. Despite the mixture of the two main groups in the Workshop, this was certainly possible in my case. These two groups were, in my eyes, not too far away from each other, so that the mixture was in the end somehow homogeneous.

From Rainer Dietmann (Royal Holloway, University of London):

I found it very good to bring together people from many different areas. For example for me, it was an excellent opportunity to talk to Lenny Fukshansky and Jeff Vaaler about small zeros of pairs of quadratic forms, to people from Analytic Number Theory (Tim Browning and Roger Heath-Brown), to algebraists such as David Leep, to modular forms people such as Rainer Schulze-Pillot who gave me some very useful references on the problem of representing quadratic forms by quadratic forms, and to other "point-counting" number theorists such as Martin Widmer. In fact, this meeting has been the most fruitful one for me for a long time.

From Roger Heath-Brown (Oxford University):

I have some thoughts on the workshop. Firstly, I felt it was the most successful meeting I've attended in the past 3 years (at least). I had been concerned that, coming from a more analytic background than most of the participants, I would find nothing of interest. In fact I came away inspired with 2 or 3 different ideas for future investigation - with most meetings the count is 0.

From David Leep (University of Kentucky):

This conference was incredibly useful to me because people from a number of different areas came together. It is always useful and wonderful to see people I already know. For example, I had excellent discussions with Jean Louis Colliot Thelene, a colleague with whom I have discussed mathematics for several decades. At this conference I explained a new theorem I proved that extended some of his work. I plan to include this theorem in the paper I will submit to the proceedings of this conference.

Besides seeing long time colleagues and acquaintances, I was able to meet a number of new people. This included people with whom I have already been in e-mail contact, but had never met, and other people with whom I have never been in contact. For example, I was quite pleased to meet Tim Browning. We had already been in e-mail contact (along with Colliot Thelene) about a paper that one of his PhD students had written. It was wonderful to meet him in person. That makes future e-mail contact much better and much more pleasant. It also makes a future visit more likely.

Perhaps the highlight of the conference for me was finally meeting Roger Heath-Brown. We have exchanged e-mail before on several topics. Roger was already familiar with some of my work. (Obviously I was already familiar with his work.) So it was a great pleasure to have conversations with him concerning some topics of mutual interest to both of us.

It was also fun meeting a number of new people, mostly younger people, and having discussions with them. I knew some of their names previously (for example Ben Kane and others) while some of their names were completely new to me. I thoroughly enjoyed the conference.

3 Presentation Highlights

Our participants presented 6 hour-long plenary talks and 16 invited 30-minute talks, which stimulated a number of lively discussions that will likely lead to new research and collaborations. The goal of some plenary talks was to survey a given subarea, while most invited talks reported on specific recent developments. We have attached the abstracts below.

3.1 Hour-long talks

Eva Bayer-Fluckiger (École Polytechnique Fédérale de Lausanne)

Title: *Galois algebras, Hasse principle and induction-restriction methods*
Abstract: Let k be a field of characteristic $\neq 2$, and let L be a Galois extension of k with group G. Let us denote by $q_L : L \times L \to k$ the *trace form*, defined by $q_L(x, y) = \mathrm{Tr}_{L/k}(xy)$. Let $(gx)_{g\in G}$ be a normal basis of L over k. We say that this is a *self–dual normal basis* if $q_L(gx, hx) = \delta_{g,h}$. If the order of G is odd, then L always has a self–dual normal basis over k (cf. [3]). This is no longer true in general if the order of G is even; some partial results are given in [4].

If k is an algebraic number field, then it is natural to ask whether a local–global principle holds for this problem. In order to make this question precise, we have to consider G–Galois algebras and not only field extensions. Moreover, it is useful to note that q_L is a G*–quadratic form*, in other words $q_L(gx, gy) = q_L(x, y)$ for all $x, y \in L$ and $g \in G$. The G–Galois algebra has a self–dual normal basis if and only if the G–form q_L is isomorphic to the unit G–form. We have the following:
Theorem. *Suppose that k is a global field of characteristic $\neq 2$. Let G be a finite group, and suppose that the fusion of the 2-Sylow subgroups of G is controlled by the fusion. Let L and L' be two G–Galois algebras such that for all places v of k, the G–forms q_{L_v} and $q_{L'_v}$ are isomorphic over k_v. Then the G–forms q_L and $q_{L'}$ are isomorphic over k.*
Corollary. *Suppose that k and G are as above. Then a G–Galois algebra has a self–dual normal basis over k if and only if such a basis exists over all the completions of k.*

The proof uses a result concerning induction and restriction for arbitrary G–quadratic forms, which is of independent interest. This is a joint work with Parimala.

J.-L. Colliot-Thélène (CNRS, Université Paris-Sud, France)

Titre de l'exposé: *Sur l'équation $q(x, y, z) = P(t)$ en entiers*
Résumé: Travail en commun avec Fei XU (Capital Normal University, Beijing, Chine).

Définition : Approximation forte hors de S

Soit X une variété algébrique sur un corps de nombres k. Soit $S \subset T$ avec T ensemble fini de places contenant les places archimédiennes et $\mathcal{X}/O_T$ un modèle de X/k sur l'anneau des T-entiers, puis pour chaque $v \in T \setminus S$, un ouvert $U_v \subset X(k_v)$. Dans toute telle situation, si l'ensemble

$$\prod_{v\in S} X(k_v) \times \prod_{v\in T\setminus S} U_v \times \prod_{v\notin T} \mathcal{X}(O_v) \subset X(\mathbf{A}_k)$$

est non vide, il contient l'image diagonale d'un point de $X(k)$.

Lorsque ceci vaut, on a un principe local-global pour les points S-entiers.

Cas classiques d'approximation forte : la droite affine (reste chinois); équation $q(x_1, \dots, x_n) = a$ avec $n \geqslant 4$, q isotrope en une place $v \in S$. (Eichler, Kneser); groupe algébrique semisimple simplement connexe G/k sous une hypothèse forte de non compacité pour $\prod_{v \in S} G(k_v)$ (Kneser, Platonov).

L'approximation forte peut être en défaut. De nombreux exemples ont été interprétés (CT-Xu, 2005–2009) en terme de l'obstruction de Brauer-Manin (qui jusque là avait plutôt été considérée dans l'étude des points rationnels).

On utilise le groupe de Brauer des schémas et l'accouplement

$$X(\mathbf{A}_k) \times \mathrm{Br}(X) \to \mathbb{Q}/\mathbb{Z}$$

$$(\{M_v\}, A) \mapsto \sum_v \mathrm{inv}_v A(M_v),$$

qui est nul sur $X(k) \times \mathrm{Br}(X)$ (loi de réciprocité de la théorie du corps de classes). On note

$$X(\mathbf{A}_k)^{\mathrm{Br}(X)}$$

le noyau à gauche. On a donc $X(k) \subset X(\mathbf{A}_k)^{\mathrm{Br}(X)}$.

Définition : Approximation forte hors de S avec condition de Brauer-Manin)

On suppose $X(\mathbf{A}_k) \neq \emptyset$. Soit $S \subset T$ avec T ensemble fini de places contenant les places archimédiennes et $\mathcal{X}/O_T$ un modèle de X/k, puis pour chaque $v \in T \setminus S$, un ouvert $U_v \subset X(k_v)$. Dans toute telle situation, si l'ensemble

$$[\prod_{v \in S} X(k_v) \times \prod_{v \in T \setminus S} U_v \times \prod_{v \notin T} \mathcal{X}(O_v)]^{\mathrm{Br}(X)} \subset X(\mathbf{A}_k)^{\mathrm{Br}(X)}$$

est non vide, il contient l'image diagonale d'un point de $X(k)$.

Théorème *L'approximation forte hors de S avec condition de Brauer-Manin vaut pour tout X/k espace homogène d'un groupe algébrique G/k linéaire connexe, avec stabilisateurs géométriques connexes, et une hypothèse convenable de non compacité aux places de S.*

Références : CT et Xu 2005-2009 (G semisimple simplement connexe); Harari 2008 (G commutatif connexe); Demarche 2011 (groupes quelconques); Borovoi et Demarche 2011 (espaces homogènes, cas général).

Que dire sur les points entiers en dehors du cadre des espaces homogènes de groupes linéaires connexes ?

Penser à la situation analogue pour l'étude du principe local-global et l'approximation faible sur les points *rationnels*. Le cas des espaces homogènes de groupes algébriques linéaires connexes (avec stabilisateur connexe) a été beaucoup étudié (Eichler, Kneser, Harder, Chernousov, Sansuc, Borovoi). On a ensuite étudié l'extension à d'autres types de variétés, en particulier les variétés X avec une fibration $\pi : X \to \mathbf{A}^1_k$ dont la fibre générale est un tel espace homogène.

Soient k un corps, $q(x, y, z)$ une forme quadratique ternaire sur k, non dégénérée, et $P(t) \in k[t]$ non nul. Notons X/k la variété affine

$$q(x, y, z) = P(t).$$

Si $P(t)$ est séparable, X est lisse. Soit $U \subset X$ l'ouvert complémentaire de $x = y = z = 0$. C'est une variété lisse. Soit $\tilde{X} \to X$ une résolution des singularités de X, avec $U \subset \tilde{X}$.

Théorème principal de l'exposé (JLCT et Fei XU, 2011)

Pour k un corps de nombres et v_0 une place de k telle que q est isotrope sur k_{v_0}, l'approximation forte hors de $S = \{v_0\}$ avec condition de Brauer-Manin vaut pour tout ouvert Zariski V de X avec $U \subset V \subset \tilde{X}$.

La condition Brauer–Manin est nécessaire, mais l'approximation forte hors de S vaut si $P(t) \neq c.(r(t))^2$ avec $c \in k^\times$.

Sinnou David (Université Pierre et Marie Curie - Paris 6)

Title: *A journey through heights: the Lehmer problem*

Abstract: After a brief description of the original Lehmer problem and the work that has been done around it till the seventies, we shall concentrate on the last decade. We shall show how the Lehmer problem can now be seen in a general geometric setup, how it interacts with aspects of global analysis, how the variation of the base field can be taken into account. We shall describe a few general conjectures that contain the original Lehmer problem as a special case and present a few recent results.

Roger Heath-Brown (University of Oxford)

Title: *p-adic zeros of systems of quadratic forms*
Abstract: This is a survey talk concerning the following problem. Let K be a field and let $r \in \mathbb{N}$. Define $\beta(r;K)$ to be the largest integer n for which there exist quadratic forms

$$q_i(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n] \quad (1 \leqslant i \leqslant r)$$

having only the trivial common zero over K. What can one say about $\beta(r;K)$, particularly in the case $K = \mathbb{Q}_p$? It is conjectured that $\beta(r;\mathbb{Q}_p) = 4r$ for all p and all r. This is known for $r = 1$ and $r = 2$.

Two lines of attack are sketched. The first uses reduction to $\mathbb{F}_p$, looks for a non-singular zero, and then applies Hensel's Lemma. This requires the use of a suitable "minimal model" for the system. The approach is successful when p is large in terms of r, and has been used by Leep to show that $\beta(1;K) = 2^{t+2}$ when $K = \mathbb{Q}_p(t_1,\ldots,t_k)$, irrespective of p. However in the case $K = \mathbb{Q}_p$ a counterexample shows that the method, at least in its simplest form, fails for $p = 2$.

The second approach uses induction on r. It provides results for all r but produces upper bounds for $\beta(r;\mathbb{Q}_p)$ which are larger than $4r$ as soon as $r \geqslant 3$. The two methods can be made to interact, and it may be shown, using Leep's result, that $\beta(3;\mathbb{Q}_p) \leqslant 16$.

Gabriele Nebe (RWTH Aachen University)

Title: *Extremal lattices and codes*
Abstract: Using invariant theory of finite complex matrix groups, Andrew Gleason has shown in his ICM talk in Nice 1970, that the minimum distance of a doubly-even self-dual binary code of length n cannot exceed $4 + 4\lfloor \frac{n}{24} \rfloor$. A similar bound has been proven by Siegel for even unimodular lattices of dimension n, where the minimum of the regular integral quadratic form is always $\leqslant 1 + \lfloor \frac{n}{24} \rfloor$. Lattices and codes achieving equality are called **extremal**. Of particular interest are extremal lattices and codes in the "jump dimensions" - the multiples of 24.

Number of extremal lattices L and codes C.

n	8	16	24	32	48	72	80	$\geqslant 3952$	$\geqslant 163,264$
C	1	2	1	5	1	?	$\geqslant 4$	0	0
L	1	2	1	$\geqslant 10^7$	$\geqslant 3$	$\geqslant 1$	$\geqslant 5$	?	0

A very intensively studied question is the existence on an extremal code of length 72. This survey talk reports on recent progress in the study of possible automorphism groups of such a code. I will also give a construction of the extremal even unimodular lattice Γ of dimension 72 I discovered in summer 2010. The existence of such a lattice was a longstanding open problem. The construction that allows to obtain the minimum by computer is similar to the one of the Leech lattice from E_8 and of the Golay code from the Hamming code (Turyn 1967). With Richard Parker we showed that the lattice Γ is indeed the unique extremal even unimodular lattice that can be obtained from the Leech lattice with this Turyn construction. Γ can also be obtained as a tensor product of the Leech lattice (realized over the ring of integers R in the imaginary quadratic number field of discriminant -7) and the 3-dimensional Hermitian unimodular R-lattice of minimum 2, usually known as the Barnes lattice. This Hermitian tensor product construction shows that the automorphism group of Γ contains the absolutely irreducible rational matrix group $(\mathrm{SL}_2(25){\times}\mathrm{PSL}_2(7)) : 2$. It also reveals an additional structure of Γ as a lattice over $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$. This leads to a 1-parametric family of quadratic forms on Γ giving rise to even $(n^2 + 5n + 5)$-modular lattice of minimum $8 + 4n$.

Jeffrey Thunder (Northern Illinois University)

Title: *Counting certain points of given height in the function field setting*
Abstract: Fix a dimension n and a degree d. It is a well-known result of Northcott that there are only finitely many points of bounded height in projective n-space that generate a number field of degree d over the rationals (or any other number field, for

that matter). The question then becomes to estimate the number of such points. Such estimates essentially all amount to some sort of elaboration on counting lattice points in some region of Euclidean space.

If one replaces the field of rational numbers with a field of rational functions in one variable over a finite field, then the analog of Northcott's result is equally valid, and again one may try to estimate the number of such points. We will explain how one can go about counting points in this situation, how the Riemann-Roch theorem can replace the lattice point estimates above, how that makes some things much simpler than the number field case, and what aspects are perhaps less clear. We will also discuss how the estimates change qualitatively depending on the relative sizes of the dimension and degree.

3.2 30-minute talks

Ricardo Baeza (Universidad de Talca)

Title: *Levels and sublevels of Dedekind rings*
Abstract: We prove a representation result for quadratic forms over polynomial rings and we apply it to show, that there exist Dedekind rings A with level $s(A) = s(K) + 1$, where K is the quotient field of A. This is joint work with Jon Arason.

Tim Browning (University of Bristol)

Title: *Square-free hyperplanes on quadrics*
Abstract: Given a polynomial with integer coefficients, the problem of determining whether or not it takes infinitely many square-free values has long been a central concern in the analytic theory of numbers. We ask what one can say when one restricts attention to polynomials whose arguments run over the integral points on an affine quadric.

For $n \geqslant 3$ let $f \in \mathbb{Z}[X_1, \dots, X_n]$ be a non-zero polynomial, let $Q \in \mathbb{Z}[X_1, \dots, X_n]$ be a non-singular indefinite quadratic form and let m be a non-zero integer, with $-m \det Q$ not equal to a square when $n = 3$. Let $Y \subset \mathbb{A}^n$ be the affine quadric $Q = m$. We seek to exhibit conditions on f under which there exist infinitely many points $\mathbf{x} \in Y(\mathbb{Z})$ for which $f(\mathbf{x})$ is square-free. In fact we are able to obtain an asymptotic formula when f is linear, as follows.

Theorem 1. *Assume that* $\deg f = 1$. *Then there exist constants* $c_Y \geqslant 0$ *and* $\delta > 0$ *such that*

$$\#\{\mathbf{x} \in Y(\mathbb{Z}) : |\mathbf{x}| \leqslant X,\ f(\mathbf{x}) \textit{ is square-free}\} = c_Y X^{n-2} + O_{\delta,f,Y}(X^{n-2-\delta}).$$

For comparison, when $n \geqslant 4$, Baker [1, 2] has used a variant of the Hardy–Littlewood circle method to study asymptotically the density of $\mathbf{x} \in Y(\mathbb{Z})$ for which each coordinate x_i is square-free. The first step in the proof of Theorem 1 uses the indicator function

$$\sum_{k^2 | N} \mu(k) = \begin{cases} 1, & \text{if } N \text{ is square-free,} \\ 0, & \text{otherwise,} \end{cases}$$

where μ is the Möbius function. For a fixed integer k this leads us to count $\mathbf{x} \in Y(\mathbb{Z})$ with $|\mathbf{x}| \leqslant X$ for which $k^2 \mid f(\mathbf{x})$. The argument bifurcates according to whether or not k is small. If k is small we use work of Gorodnik and Nevo [6], based on dynamical systems and mixing, to analyze the relevant counting problem. If k is large we transform the problem into one that involves counting integral points on suitable affine quadrics.

Suppose we are given a non-zero quadratic polynomial $q \in \mathbb{Z}[T_1, \dots, T_\nu]$, with quadratic part q_0, for $\nu \geqslant 2$. Consider the counting function

$$M(q; B) = \#\{\mathbf{t} \in \mathbb{Z}^\nu : q(\mathbf{t}) = 0,\ |\mathbf{t}| \leqslant B\},$$

for any $B \geqslant 1$. We will require an upper bound for $M(q; B)$ which is uniform in the coefficients of q and which is essentially as sharp and as general as possible. A trivial estimate is $M(q; B) = O_\nu(B^{\nu-1})$, which is as good as can be hoped for when q is reducible over $\mathbb{Q}$. Assuming that q is irreducible over $\mathbb{Q}$, a result of Pila [7] reveals that $M(q; B) = O_{\varepsilon,\nu}(B^{\nu-3/2+\varepsilon})$, for any $\varepsilon > 0$. Again this is essentially best possible when $\operatorname{rank}(q_0) = 1$, as consideration of the polynomial $T_1 - T_2^2$ shows. For the remaining cases we establish the following improvement.

Theorem 2. *Assume that q is irreducible over $\mathbb{Q}$ and that $\operatorname{rank}(q_0) \geqslant 2$. Then we have $M(q;B) = O_{\varepsilon,\nu}(B^{\nu-2+\varepsilon})$, for any $\varepsilon > 0$.*

The most important feature of Theorem 2 is its uniformity in the coefficients of the quadratic polynomial q. It reflects the rough order of magnitude of $M(q;B)$ when $q = q_0$. The result is proved by induction on ν, the case $\nu = 2$ essentially going back to work of Estermann. This is joint work with A. Gorodnik.

Renaud Coulangeon (University of Bordeaux)

Title: *The unreasonable effectiveness of tensor product*

Abstract: An extremal even unimodular lattice in dimension 72 was recently constructed by Gabriele Nebe, elaborating on ideas of Robert Griess. This lattice appears rather naturally as a tensor product over an imaginary quadratic ring of two lattices of lower dimension. Similar tensor constructions of extremal modular lattices in dimension 40 and 80 had already been proposed by Christine Bachoc and Gabriele Nebe in 1998. In this talk, I will first explain why one should not expect, in general, to produce dense lattices using tensor product and try then to analyze the very special features of the above mentioned constructions which explain their “unreasonable effectiveness”. In a different direction, I will also report on an intriguing conjecture by Jean-Benoît Bost which predicts a very rigid behavior of so-called semi-stable lattices with respect to tensor product.

Rainer Dietmann (Royal Holloway, University of London)

Title: *Weyl’s inequality and systems of forms*

Abstract: Whereas for one single quadratic form or a pair of quadratic forms a variety of approaches from areas such as modular forms or arithmetic geometry have been successfully applied, for systems of more than two quadratic forms Hardy-Littlewood’s circle method still seems to be the most powerful tool. In our talk we explained how one can give the basic form of Weyl’s inequality in Birch’s seminal work ([5]) on forms in many variables a more efficient interpretation for systems of forms. As an application, we can improve results by W.M. Schmidt ([9], [10]) on systems of quadratic and systems of cubic forms, replacing $2r^2 + 3r$ by $2r^2 + 2r$ and $10r^2 + 6r$ by $8r^2 + 8r$, respectively.

Theorem 1. *Let $Q_1, \ldots, Q_r \in \mathbb{Z}[X_1, \ldots, X_s]$ be quadratic forms, such that each form in their rational pencil has rank exceeding $2r^2 + 2r$. Then if $\mathfrak{N}(P)$ denotes the number of common integer zeros of $Q_1, \ldots, Q_r$ in an expanding box of size P, then*

$$\mathfrak{N}(P) = \mathfrak{J}\mathfrak{S}P^{s-2r} + O(P^{s-2r-\delta})$$

holds true, where $\mathfrak{J}$ and $\mathfrak{S}$ are the singular integral and the singular series, respectively. Likewise, if $C_1, \ldots, C_r \in \mathbb{Z}[X_1, \ldots, X_s]$ are cubic forms, such that each form in their rational pencil has h-invariant exceeding $8r^2 + 8r$, then

$$\mathfrak{N}(P) = \mathfrak{J}\mathfrak{S}P^{s-3r} + O(P^{s-3r-\delta}).$$

Moreover, we discussed the closely related problem of representing quadratic forms by quadratic forms: Let A be a non-singular positive definite symmetric integer $n \times n$-matrix, and B be a positive definite symmetric integer $m \times m$-matrix, and let $N(A,B)$ be the number of integer solutions X of the matrix equation

$$X^t AX = B. \tag{1}$$

Using Siegel modular forms, Raghavan ([8]) obtained an asymptotic formula for $N(A,B)$ if $n > 2m+2$, $\min B \gg (\det B)^{1/m}$ and $\det B$ is large enough. Writing (1) as a system of quadratic equations, this problem can also be attacked by the circle method. The following preliminary result (work in progress) has been obtained in joint work with Michael Harvey.

Theorem 2. *Let $c > 0$ and suppose that*

$$\min B \geqslant (\det B)^c.$$

Then there exists $N(c) \in \mathbb{N}$ such that if $n \geqslant N(c)$ and $\det B \gg_c 1$, then

$$N(A,B) = \mathfrak{J}\mathfrak{S}(\det B)^{(n-m-1)/2} + O((\det B)^{(n-m-1)/2-\delta}).$$

The assumption on the dimension n now has become worse than in Raghavan's result, but the interesting feature here is that the assumption on the right-hand side B is less restrictive, showing that the circle method and the modular forms approach each have their strengths and weaknesses for this problem and yield complementary results.

Jonathan Hanke (University of Georgia)

Title: *Understanding the (total) mass of quadratic forms of fixed determinant*
Abstract: The mass of a genus of quadratic forms is a very useful invariant that is closely related to the class number, but can also be computed by purely local methods. In this talk we describe the structure of the somewhat coarser invariant called the total mass

$$\text{TMass}_n(D) := \sum_{\substack{\text{classes } [Q] \text{ with } Q>0, \\ \det_H(Q)=D \text{ and } \dim(Q)=n}} \frac{1}{\#\text{Aut(Q)}} = \sum_{\substack{\text{pos. def. genera G with} \\ \det_H(G)=D \text{ and } \dim(G)=n}} \text{Mass}(G)$$

which is defined to be the sum of all masses of genera G of positive definite integer-valued quadratic forms of Hessian determinant D in n variables, and give an exact formula for $\text{TMass}_n(D)$ when $n = 3$. The total mass is closely related to the asymptotics of certain arithmetic parametrizations of Bhargava which count the classes of ternary quadratic forms by their unique polynomial invariant (the discriminant!).

Ben Kane (University of Cologne)

Title: *Representations by triangular, square, and pentagonal sums*
Abstract: Fermat claimed that all positive integers are represented by 3 triangular numbers, 4 squares, 5 pentagonal, . . . , and m m-gonal numbers. Its determination in the cases $m = 4$ (resp. $m = 3$) was celebrated work of Lagrange (resp. Gauss) and the full conjecture was finally resolved by Cauchy in 1813. In this talk, we will discuss the related question of which "weighted sums" represent all but finitely many positive integers, with a focus on complications which first arise in the $m = 5$ case. This is based on ongoing joint work with W.K. Chan and A. Haensch.

Abhinav Kumar (Massachusetts Institute of Technology)

Title: *Energy minimization for lattices and periodic configurations, and formal duality*
Abstract: Closely related to the sphere packing problem is the energy minimization problem for discrete sets of points in Euclidean space, which can be reformulated as an optimization problem for the (average) theta function. I will describe some numerical experiments (joint work with Henry Cohn and Achill Schuermann) which gives evidence for the energy minimizing periodic configurations in low dimensions, for Gaussian potential energy. Surprisingly, the putative optimizers are not necessarily lattices, but appear in families exhibiting formal duality.

Byeong-Kweon Oh (Seoul National University)

Title: *Class numbers of ternary quadratic forms*
Abstract: Let L be a positive definite ternary $\mathbf{z}$-lattice. We define

$$\Lambda_p(L) = \{x \in L \mid Q(x+z) \equiv Q(z) \pmod{ep} \text{ for all } z \in L\},$$

where $e = 2$ if L is even and $p = 2$, otherwise $e = 1$. The $\mathbf{z}$-lattice $\lambda_p(L)$ is the primitive $\mathbf{z}$-lattice obtained from $\Lambda_p(L)$ by a suitable scaling. Let K be a ternary $\mathbf{z}$-lattice. If a $\mathbf{z}$-lattice L satisfies $K = \prod_{p_i|2dL} \lambda_{p_i}^{m_i}(L)$ for some suitable m_i, we say L is lying over K. In this case we define

$$\text{gen}^K(L) := \{L' \in \text{gen}(L) : \prod_{p_i|2dL} \lambda_{p_i}^{m_i}(L') \simeq K\}.$$

We denote by $h^K(L)$ the number of equivalence classes in $\text{gen}^K(L)$. Note that $h(L) = \sum_{K' \in \text{gen}(K)/\sim} h^{K'}(L)$. Let M be a ternary $\mathbf{z}$-lattice. If $\sigma = \tau_x \in O(M)$ for a primitive vector $x \in M$, we define $\pi(\sigma, M) := Q(x)$. If $\sigma_1, \dots, \sigma_t$ are all symmetries in $O(M)$, we define **the signature of** M as follows:

$$\text{sgn}(M) = \langle o(M); \pi(\sigma_1, M), \pi(\sigma_2, M), \dots, \pi(\sigma_t, M) \rangle.$$

Assume that $\lambda_p(L) = K$ and p is an odd prime. In this talk we prove the following theorem:

Theorem. *The number of equivalence classes in gen*$^K(L)$ *having an isometry group with given order, and the signature of each lattice in gen*$^K(L)$ *are completely determined by the signature of* K *(also the structure of* L_p *and* K_p*).*

From the above theorem, we can inductively compute $h^K(M)$ for any lattice M lying over K if we only know the signature of K. For example, let $K = \mathbf{z}x_1 + \mathbf{z}x_2 + \mathbf{z}x_3$ be ternary $\mathbf{z}$-lattice such that

$$(B(x_i, x_j)) = \begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 7 \end{pmatrix}.$$

Note that the class number of K is one. Define $K(7^n) = \mathbf{z}x_1 + \mathbf{z}x_2 + \mathbf{z}(7^n x_3)$. If we use the above theorem, we can easily compute $h(K(7^n)) = 3 \cdot 7^{2n-2} + 2 \cdot 7^{n-1} - \frac{3}{8}(7^{2n-2} - 1)$. This is a joint work with W. K. Chan from Wesleyan University.

Bruce Reznick (University of Illinois at Urbana Champaign)

Title: *Linear dependence among powers of quadratic forms*

Abstract: Let $\Phi(d)$ be the smallest r so that there exist r pairwise non-proportional complex quadratic forms $\{q_i\}$ with the property that $\{q_i^d\}$ is linearly dependent.

Problem: compute $\Phi(d)$ and characterize the minimal sets. Any set of $2r + 2$ q_i^d's is dependent, so $\Phi(d) \leqslant 2d + 2$, but a "general" set of $2r + 1$ q_i^d's is linearly independent.

The Pythagorean parameterization gives the unique minimal set up to change of variable: $\Phi(2) = 3$ and $(x^2 - y^2)^2 + (2xy)^2 = (x^2 + y^2)^2$. Liouville's proof of Fermat's Last Theorem for non-constant polynomials implies that for $d \geqslant 3$, $\Phi(d) \geqslant 4$. A deep theorem of Mark Green implies that $\Phi(d) \geqslant 1 + \sqrt{d+1}$. In the other direction, many 19th century examples show that $\Phi(3) = \Phi(4) = \Phi(5) = 4$. New results: a characterization of the minimal sets for $d \leqslant 5$; if $d \geqslant 6$, then $\Phi(d) \geqslant 5$, $\Phi(6) = \Phi(7) = 5$, $\Phi(14) \leqslant 6$; $\Phi(d) \leqslant 2 + \lfloor d/2 \rfloor$ if $d \geqslant 4$.

My work on this was motivated by a 1999 seminar of Bruce Berndt about an question of Ramanujan, who wanted a generalization of the identity of the form $f_1^3 + f_2^3 = f_3^3 + f_4^3$ for four specific quadratic forms in $\mathbb{Z}[x, y]$. Neither Ramanujan, nor Narayanan, who solved his question, noted that there existed other quadratic forms f_j so that $f_1^3 + f_2^3 = f_3^3 + f_4^3 = f_5^3 + f_6^3$ and $f_1^3 - f_4^3 = f_3^3 - f_2^3 = f_7^3 + f_8^3$, but nothing further for $f_1^3 - f_3^3 = f_4^3 - f_2^3$. This is typical. For $\alpha \in \mathbb{C}$,

$$(\alpha x^2 - xy + \alpha y^2)^3 + \alpha(-x^2 + \alpha xy - y^2)^3 = (\alpha^2 - 1)(\alpha x^3 + y^3)(x^3 + \alpha y^3),$$

and if $y \mapsto \omega y$, where $\omega^3 = 1$, then the right-hand side is unchanged, hence there are two other pairs of quadratic forms whose cubes which have the same sum. Up to change of variable, these are *all* the minimal solutions of degree 3. In some cases, solutions coalesce: $x^6 + y^6$ is a sum of two cubes in four different ways and $xy(x^4 + y^4)$ in six ways. There are three different minimal solutions of degree 4 and one of degree 5, but no families of solutions, as there are in degree 3.

Felix Klein promoted the idea of associating each linear form $x - \alpha y$, $\alpha \in \mathbb{C}$ with the image of α on the Riemann map from $\mathbb{C}$ to the unit sphere (and y to the north pole.) We associate quadratic forms to the *pairs* of points of their factors. In this way, the Pythagorean parameterization corresponds to antipodal pairs of the vertices of an octahedron, the unique solution for $d = 5$ corresponds to antipodal pairs of the vertices of a cube and the example for $d = 14$ corresponds to antipodal pairs of the vertices of a regular icosahedron. This cannot be an accident. In every known minimal solution $\{q_j\}$, there is a change of variables after which, $|\alpha_j| = |\gamma_j|$ in each $q_j(x, y) = \alpha_j x^2 + \beta_j xy + \gamma_j y^2$.

It's useful to consider sums of the form $\sum_{k=0}^{m-1} (\zeta_m^k x^2 + \beta xy + \zeta_m^{-k} y^2)^d$ where $\zeta_m = e^{2\pi i/m}$ and $m > 2d$; the sum on roots of unity kills the coefficient of all terms but $x^{d \pm m} y^{d \mp m}$ and $x^d y^d$, and β is chosen to leave a multiple of $(xy)^d$. In this way, one can show that $\Phi(d) \leqslant 2 + \lfloor d/2 \rfloor$ if $d \geqslant 4$, although this is not best possible for $d = 14$. These sets of quadratic forms have a Klein correspondence with a polyhedron whose vertices are the two poles and two antipodal horizontal m-gons.

Damien Roy (University of Ottawa)

Title: *On rational approximation to real points on plane quadratic curves defined over* $\mathbb{Q}$
Abstract: A point (ξ_1, ξ_2) with coordinates in a subfield of $\mathbb{R}$ of transcendence degree one over $\mathbb{Q}$, with $1, \xi_1, \xi_2$ linearly independent over $\mathbb{Q}$, may have a uniform exponent of approximation by elements of $\mathbb{Q}^2$ that is strictly larger than the lower bound $1/2$ given by Dirichlet's box principle. This appeared as a surprise, in connection to work of Davenport and Schmidt, for points of the parabola $\{(\xi, \xi^2)\,;\, \xi \in \mathbb{R}\}$. The goal of this talk is to show that this phenomenon extends to all real conics defined over $\mathbb{Q}$, and that the largest exponent of approximation achieved by points of these curves satisfying the above condition of linear independence is always the same, independently of the curve, namely $1/\gamma \cong 0.618$ where γ denotes the golden ratio.

Rudolf Scharlau (Universität Dortmund)

Title: *Automorphism groups of lattices in large genera*
Abstract: In fixed dimension n, almost all lattices (with primitive integral quadratic forms) of determinant d have trivial automorphism groups when $d \to \infty$. This is a well known, classical consequence of reduction theory. The lattices of any given dimension and determinant split into genera, and in the thesis of J. Biermann (Göttingen, 1981) it had been shown that the result also holds for the lattices of any genus. Since the mass and the class number of genera tend to infinity also with the dimension n, one might expect that the result more sharply holds if $\max(n, d) \to \infty$. That is, only finitely many genera might exceed a specified proportion of lattices with non-trivial group. This is far from being proved. In the talk, we shall be more modest and report on explicit, computational results on the automorphism groups actually occurring for arithmetically interesting genera of dimension up to 20 and small level. Roughly speaking one observes that for these parameters (the level seems to be more appropriate than the absolute size of the determinant), automorphism groups are still a good invariant. On the other hand, when the level 1,2,3,4,5,6,7,11 goes up, the quick increase of the mass is mostly caused by a quick increase of the number of lattices with very small, eventually trivial automorphism group.

Achill Schürmann (Universität Rostock)

Title: *Strictly periodic extreme lattices*
Abstract: A lattice is called periodic extreme if it cannot locally be modified to yield a better periodic sphere packing. It is called strictly periodic extreme if it gives an isolated local optimum among periodic sphere packings. We derive sufficient conditions for periodic extreme and strictly periodic extreme lattices. We hereby in particular show that the root lattice E_8, the Coxeter-Todd lattice K_{12}, the Barnes-Wall lattice BW_{16} and the Leech lattice Λ_{24} are strictly periodic extreme.

Cameron Stewart (University of Waterloo)

Title: *Exceptional units and cyclic resultants*
Abstract: Let a be a nonzero algebraic integer of degree d over the rationals. Put $K = \mathbb{Q}(a)$ and let $\mathcal{O}(K)$ denote the ring of algebraic integers of K. We shall discuss estimates for the number of positive integers n for which $a^n - 1$ is a unit in $\mathcal{O}(K)$ and for the largest positive integer n for which $a^j - 1$ is a unit for j from 1 to n.

Takao Watanabe (Osaka University)

Title: *Polyhedral reduction of Humbert forms over a totally real number field*
Abstract: Let k be a totally real number field and o the ring of integers of k. We write $\mathsf{k}_{\mathbf{R}}$ for $\mathsf{k} \otimes_{\mathbf{Q}} \mathbf{R}$. Let $H_n(\mathsf{k}_{\mathbf{R}})$ be the space of all $n \times n$ symmetric matrices with entries in $\mathsf{k}_{\mathbf{R}}$ and $P_n(\mathsf{k}_{\mathbf{R}}) = \{{}^t gg \mid g \in GL_n(\mathsf{k}_{\mathbf{R}})\}$ be an open cone in $H_n(\mathsf{k}_{\mathbf{R}})$. The rational closure Ω_{k} of $P_n(\mathsf{k}_{\mathbf{R}})$ is defined to be the cone generated by $\{x^t x \mid x \in \mathsf{k}^n \setminus \{0\}\}$ in $H_n(\mathsf{k}_{\mathbf{R}})$. Our purpose is to study polyhedral reduction of $\Omega_{\mathsf{k}}/GL(\Lambda)$ for a given projective o-module $\Lambda \subset \mathsf{k}^n$ of rank n.

We define the Λ-minimum function $\mathsf{m}_\Lambda \,:\, P_n(\mathsf{k}_{\mathbf{R}}) \longrightarrow \mathbf{R}_{\geqslant 0}$ by

$$\mathsf{m}_\Lambda(a) = \inf_{0 \neq x \in \Lambda} \mathrm{Tr}_{\mathsf{k}_{\mathbf{R}}/\mathbf{R}}({}^t xax)\,.$$

The domain $K_1(\mathsf{m}_\Lambda) = \{a \in P_n(\mathsf{k}_{\mathbf{R}}) \mid \mathsf{m}_\Lambda(a) \geqslant 1\}$ gives an analog of Ryshkov polyhedron. Indeed, $K_1(\mathsf{m}_\Lambda)$ is a locally finite polyhedron. Let $\partial^0 K_1(\mathsf{m}_\Lambda)$ be the set of all vertices of $K_1(\mathsf{m}_\Lambda)$. By extending Voronoï's algorithm to $K_1(\mathsf{m}_\Lambda)$, we obtain a complete set $\{b_1, \cdots, b_t\}$ of representatives of $\partial^0 K_1(\mathsf{m}_\Lambda)/GL(\Lambda)$.

For $a \in \partial^0 K_1(\mathsf{m}_\Lambda)$, the perfect cone D_a is defined to be the closed cone in $H_n(\mathsf{k}_{\mathbf{R}})$ generated by $\{x^t x \mid x \in S_\Lambda(a)\}$, where $S_\Lambda(a)$ stands for the set of minimal vectors of a in Λ. Then we can show that the set of all perfect cones gives a polyhedral subdivision of Ω_k, and hence the domain

$$\bigcup_{i=1}^{t} D_{b_i}/\Gamma_i$$

gives a fundamental domain of $\Omega_\mathsf{k}/GL(\Lambda)$, where Γ_i denotes the stabilizer of b_i in $GL(\Lambda)$.

If $n = 1$ and $\Lambda = \mathsf{o}$, then this result may be regarded as a precise form of Shintani's unit theorem for the square E_k^2 of the unit group $E_\mathsf{k} = GL_1(\mathsf{o})$. In the case that k is a quadratic field, $K_1(\mathsf{m}_\mathsf{o})$ is a polygonal region in $\mathbf{R}^2_{>0}$ with infinite vertices. We see that there are many real quadratic fields such that the number of elements of $\partial^0 K_1(\mathsf{m}_\mathsf{o})/E_\mathsf{k}$ is equal to one.

Mark Watkins (University of Sydney)

Title: *Indefinite LLL and solving quadratic equations*
Abstract: This talk reviews work on modifying the LLL algorithm so that it would apply to indefinite symmetric matrices, and noted Simon's attempts (dating from 2005) to further apply this to solve quadratic equations (thus generalizing the 3-variable conic case known to Gauss). The question of finding a solution space of maximal dimension was also considered, as was the generality of an idea of Cassels (adapted by Simon) in various circumstances. The practicality of the algorithms appears evident, with only the factorizing of the determinant preventing the algorithm from running in polynomial time. The quite recent work of Castel on solving an indefinite form of dimension 5 *without* factorizing the discriminant was also mentioned briefly.

Martin Widmer (Graz University of Technology)

Title: *Integral points of fixed degree and bounded height*
Abstract: In Jeff Thunder's talk we have considered the number of algebraic points of bounded height and of fixed degree over a given global field k. By Northcott's Theorem it is known that these points are finite in number, and the emphasis of Thunder's talk was to find the asymptotics as the height bound becomes large. In this talk we consider a closely related problem. Let k be a number field, let n and e be positive rational integers, and let $X > 1$ be real. We consider the algebraic points $(\alpha_1, ..., \alpha_n)$ of affine Weil height at most X such that each coordinate is an algebraic integer, and such that they generate an extension $k(\alpha_1, ..., \alpha_n)$ of k of degree e.

We present a precise asymptotic estimate for their number (as X tends to infinity) involving several main terms of decreasing order. We outline the proof in the much simpler special case $e = 1$ where one has to count lattice points in an unpleasant shaped subset S of the Euclidean space $\mathbb{R}^m$. Here a crucial ingredient of the proof is a gap principle for the successive minima of a lattice under a certain subgroup $\mathcal{M}$ of the diagonal endomorphisms. Loosely speaking it says that we can replace our set S by $\Phi(S)$ for any element Φ of $\mathcal{M}$, essentially without changing the number of lattice points. This principle might have applications to other counting problems.

References

[1] R.C. Baker, The values of a quadratic form at square-free points. *Acta Arith.* **124** (2006), 101–137.

[2] R.C. Baker, The zeros of a quadratic form at square-free points. *J. Number Theory* **130** (2010), 2119–2146.

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

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

[5] B.J. Birch, Forms in many variables, *Proc. Royal Soc. A* **265** (1962), 245–263.

[6] A. Gorodnik and A. Nevo, Counting lattice points. *J. Reine Angew. Math.*, to appear.

[7] J. Pila, Density of integral and rational points on varieties. *Astérisque* **228** (1995), 183–187.

[8] S. Raghavan, Modular forms of degree n and representation by quadratic forms, *Ann. of Math.* **70** (1959), 446–477.

[9] W.M. Schmidt, Simultaneous rational zeros of quadratic forms, Seminar of Number Theory, Paris 1980–81, *Progr. Math.* **22** (1982), 281–307.

[10] W.M. Schmidt, On cubic polynomials. IV. Systems of rational equations, *Monatsh. Math.* **93** (1982), 329–348.