# RESEARCH STATEMENT

VÍTĚZSLAV KALA

I like working on a variety of problems that combine techniques from algebra and geometry to study and count objects of number-theoretic significance.

In this proposal I mention three areas in which I have been recently involved: Section 1 talks about the question of the existence of universal quadratic forms over number fields. Section 2 is devoted to some quantitave results in the Langlands program related to self-dual representations. Finally, in Section 3 I discuss the solvability of Diophantine equations in certain weak models of arithmetic.

I have also worked on other problems, such as congruences for Maass forms [BCGK], and the structure of lattice-ordered groups [Ka3] and simple semirings [JKK]. This last topic has recently gained interest also thanks to its connection to non-commutative geometry [Le] which promises very interesting generalizations and applications.

Among my other current projects are the study of growth of class numbers in certain families of real quadratic fields with Dahl [DK], and the existence of orthogonal matrices with given Smith normal form with Maga [KM].

## 1. Universal quadratic forms over number fields

The study of universal quadratic forms can be said to have started in 1770 with the four square theorem of Lagrange, which one can formulate as the statement that the positive definite form $x^2+y^2+z^2+w^2$ is *universal*, i.e., that it represents every positive integer. This has been followed by a large number of further results, in some sense culminating with the Bhargava-Hanke [BH] 290-theorem that a posive definite form with integral coefficients is universal if and only if it represents $1, 2, 3, \ldots, 290$.

Universal quadratic forms have also been investigated over (totally real) number fields: In the following we consider a real quadratic field $K=\mathbb{Q}(\sqrt{D})$ for a squarefree positive integer $D$. We denote the ring of integers of $K$ by $\mathcal{O}_K$, and the conjugate of $\alpha = x+y\sqrt{D} \in K$ by $\alpha' = x-y\sqrt{D}$. By an *$M$-ary quadratic form over $K$* we mean a function

$$Q(x_1,\ldots,x_M) = a_{11}x_1^2 + a_{12}x_1x_2 + a_{22}x_2^2 + \cdots = \sum_{1\le i\le j\le M} a_{ij}x_ix_j \text{ with } a_{ij}\in\mathcal{O}_K;$$

we can also form its conjugate $Q' = \sum_{1\le i\le j\le M} a'_{ij}x_ix_j$. A form $Q$ is *totally positive* if $Q$ and $Q'$ are positive definite quadratic forms (over $\mathbb{R}$). A form $Q$ *represents* an integer $\alpha\in\mathcal{O}_K$ if there are $\alpha_1,\ldots,\alpha_M\in\mathcal{O}_K$ such that $Q(\alpha_1,\ldots,\alpha_M)=\alpha$, and the form is *universal* if it represents all totally positive integers.

Chan, Kim, and Raghavan [CKR] determined all totally positive universal ternary quadratic forms over $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{5})$ and showed in addition that no other real quadratic number field admits totally positive universal ternary quadratic forms. The proof uses, among other things, a theorem of Siegel [Si] which states that in no totally real field other than $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$, every totally positive integer is a sum of *any* number of squares. This is a first indication that more complicated fields might admit fewer universal quadratic forms. Kim [Ki1] showed that for squarefree $D\ge 38446$, the field $\mathbb{Q}(\sqrt{D})$ admits no diagonal 7-ary universal form (i.e., forms with $a_{ij}=0$ for all $i\ne j$),

and he also constructed an infinite family of fields of the form $\mathbb{Q}(\sqrt{n^2-1})$ admitting positive diagonal 8-ary universal forms [Ki2].

These results suggest the following natural question: Is there a common bound $M$ such that every totally real number field $K$ has a universal form in $M$ variables?

In a recent joint work with Valentin Blomer we proved that the answer is "No!":

**Theorem 1** ([BK], [Ka]). *For each positive integer $M$ there are infinitely many real quadratic fields $\mathbb{Q}(\sqrt{D})$ which do not admit $M$-ary totally positive universal quadratic forms.*

The proof is based on the observation that if a totally positive integer $\alpha$ has small norm, then it is not a sum of totally positive integers, and so the only way how it can be represented by a quadratic form is if it appears as the coefficient of some monomial $\alpha x_i^2$. Hence it suffices to produce many such elements of small norms, which we do by considering finite approximations $\frac{p_j}{q_j}$ to the continued fraction expansion $\sqrt{D} = [u_0, \overline{u_1, u_2, \dots, u_{s-1}, 2u_0}]$. The original paper [BK] dealt very explicitly with fractions of the form $\sqrt{D} = [u_0, \overline{u, \dots, u, 2u_0}]$ and required many pages of tedious and delicate estimates of the sizes of the elements $p_i + q_i\sqrt{D}$. Later I have realized [Ka] that one can side-step these technicalities by working with a different class of continued fractions, which greatly simplifies the arguments and in fact implies a slightly more general theorem.

Another very interesting problem is that of constructing universal forms – in a work in progress with Blomer we again use continued fractions to describe a general construction that works over any real quadratic field $K = \mathbb{Q}(\sqrt{D})$ and gives an upper bound on the minimal possible number of variables. We would like to also improve our previous lower bounds to show that the lower and upper bounds are asymptotically optimal.

An intriguing generalization is to consider what happens over fields of higher degree. This is a hard problem (in fact, I am not aware of almost any previous results in this direction), but still it is possible to at least partly use similar techniques. Together with my Bachelor's student Svoboda we have recently managed to extend Theorem 1 to the case of biquadratic fields. In general, the main obstacle is that continued fractions are much less useful than in the real quadratic case.

## 2. Density of self-dual automorphic representations

The Langlands program provides a common framework for a large part of number theory. It is centered around conjectural correspondences between automorphic forms, Galois representations, and Shimura varieties. These correspondences are expected to preserve many fundamental properties of the objects involved, most notably $L$-functions and $\varepsilon$-factors.

The Langlands' reciprocity conjecture asserts that when $G$ is a connected reductive group defined over a global field $F$, automorphic representations of $G(\mathbb{A}_F)$ are expected to correspond to representations $\varphi : L_F \to {}^L G$, where ${}^L G$ is the complex $L$-group defined using the dual root datum of $G$ and $L_F$ is a conjectural extension of the absolute Galois group of $F$. There is a similar conjecture over local fields, parametrizing irreducible admissible representations of $G(F)$. In this case, we can take $L_F = W_F'$ to be the Weil-Deligne group.

Globally we do not have the group $L_F$, but assuming its existence, we can obtain a conjectural map of automorphic representations between two reductive groups $G_1$ and $G_2$ as follows: given a homomorphism $f : {}^L G_1 \to {}^L G_2$, we can compose the "Galois"

representation $\varphi : L_F \to {}^L G_1$ with $f$ to obtain $f \circ \varphi : L_F \to {}^L G_2$. The reciprocity conjecture then suggests that to $\varphi$ and $f \circ \varphi$ should correspond automorphic representations on $G_1$ and $G_2$, respectively. This gives us a conjectural map of automorphic representations from $G_1$ to $G_2$, referred to as the Langlands' principle of functoriality. It is still unknown except for some (important!) special cases, including the Jacquet-Langlands correspondence between $GL_N$ and central division algebras. In my work I use the case of lifts from classical groups to $GL_N$, proved in full generality by Arthur [Ar] using the twisted trace formula.

Let us now for simplicity take $F = \mathbb{Q}$ and $G$ a classical group, by which we shall mean a split orthogonal or symplectic group $SO_N$ or $Sp_{2n}$, or a quasi-split even orthogonal group $SO^*_{2n}$ attached to a quadratic extension $F/\mathbb{Q}$. The dual group of $G$ is again an orthogonal or symplectic group, which naturally embeds in a general linear group. For example, the dual group of $Sp_{2n}$ is $SO_{2n+1}(\mathbb{C}) \hookrightarrow GL_{2n+1}(\mathbb{C})$, and so by functoriality, automorphic representations of $Sp_{2n}(\mathbb{A}_\mathbb{Q})$ lift to automorphic representations of $GL_{2n+1}(\mathbb{A}_\mathbb{Q})$.

The image of these functorial lifts consists exactly of self-dual representations, as was proved by the descent method of Ginsburg, Rallis, and Soudry [GRS] combined with the converse theorem approach of Cogdell, Kim, Piatetski-Shapiro, and Shahidi [CKPS].

In this way, self-dual representations play an important role in the Langlands program. However, being self-dual is a fairly restrictive condition. Thus we may ask how many self-dual representations there are? Do they have density zero among all representations?

Rohrlich [Ro] has studied this question on the Galois side and proved that the density is indeed zero for representations $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_N(\mathbb{C})$ when $N = 1$ or 2 and obtained some conditional results for $N = 3$.

In my PhD thesis I focus on the density of self-dual automorphic representations [Ka2]. A convenient way of counting them is given by Weyl's law, which provides the asymptotics for the number of automorphic forms having bounded Laplacian eigenvalue and a vector fixed by a given compact subgroup. In the context of number theory, Weyl's law was originally proved and used by Selberg to show the existence of Maass forms. For $GL_N(\mathbb{A}_\mathbb{Q})$, it is due to Müller:

**Theorem 2** (Weyl's law, [Mu])**.** *For an automorphic representation $\Pi$, denote $\lambda(\Pi)$ its Laplacian eigenvalue. Fix a compact subgroup $K = K_m K_\infty$ of $GL_N(\mathbb{A}_\mathbb{Q})$, where $K_m$ is the principal congruence subgroup of level $m$ and $K_\infty = O(N)$. For $\lambda \in \mathbb{R}$, let $N(\lambda) = \sum_{\lambda(\Pi) \leq \lambda} \dim \Pi^K$, where the sum is over all cuspidal automorphic representations of $GL_N(\mathbb{A}_\mathbb{Q})$ with Laplacian eigenvalue at most $\lambda$. Then*

$$N(\lambda) = \frac{\mathrm{vol}(X)}{(4\pi)^{D/2}\Gamma(D/2+1)}\lambda^{D/2} + o(\lambda^{D/2}),$$

*where $X$ is the symmetric space $(GL_N(\mathbb{Q})\mathbb{R}_{>0})\backslash GL_N(\mathbb{A}_\mathbb{Q})/K$ and $D$ is its dimension.*

Analogously, I am interested in the same sum, but ranging only over *self-dual* cuspidal automorphic representations of $GL_N(\mathbb{A}_\mathbb{Q})$, denoted by $N_{sd}(\lambda)$.

**Theorem 3.** [Ka2] *There are positive constants $c$ and $C$ such that for all sufficiently large $\lambda$ we have $c\lambda^{d/2} < N_{sd}(\lambda) < C\lambda^{d/2}$, where $d \leq D$ is the dimension of a suitable symplectic or orthogonal symmetric space.*

In fact, if $N \neq 2$, then $d < D$ and self-dual representations have density zero among all cuspidal automorphic representations, whereas they have positive density when $N = 2$. This exception is due to the fact that $SO_3 = PGL_2$ – the lifts from this group to $GL_2$ provide for the positive proportion of self-dual representations.

Let us now take $N \neq 2$. The idea of the proof is to consider the descent $\pi$ of each self-dual $\Pi$ to one of the classical groups $G(\mathbb{A}_{\mathbb{Q}})$. I then need to relate the relevant properties of $\Pi$ and $\pi$.

The Laplacian eigenvalue of an automorphic representation $\sigma$ is determined by the infinitesimal character of the real component $\sigma_\infty$. For real groups we have the Langlands reciprocity, and so we can relate the infinitesimal characters of $\pi$ and $\Pi$ via properties of the associated parameter $\varphi : W_{\mathbb{R}} \to {}^L G \hookrightarrow {}^L GL_N$. We conclude that the infinitesimal character, and hence also the Laplacian eigenvalue, are essentially preserved under functoriality.

**Proposition 4.** *If $\Pi$ has Laplacian eigenvalue $\Lambda$, then the Laplacian eigenvalue of $\pi$ is $\lambda = c_G \Lambda + d_G$ for constants $c_G > 0$ and $d_G$ (depending on $G$, but not on $\Pi$ and $\pi$).*

I also need to relate the compact subgroups for $\pi$ and $\Pi$. This is a purely local question, but it is still quite involved, Using the local notion of depth I can show:

**Proposition 5.** *For each $M \in \mathbb{N}$ there is $m \in \mathbb{N}$ such that if $\Pi$ has a vector fixed by $K_M K_\infty$, then $\pi$ has a vector fixed by $K'_m K'_\infty$, where $K'_m$ is the principal congruence subgroup of level $m$ in $G(\mathbb{A}_{\mathbb{Q},fin})$ and $K'_\infty$ is a maximal compact subgroup in $G(\mathbb{R})$.*

It is expected that depth is preserved under Langlands functoriality and reciprocity in quite a great generality. The proof of the previous proposition is based on a weak version of this relation.

Now to prove the upper bound in Theorem 3, I need to estimate $N_{sd}(\lambda)$. Each of the counted self-dual representations $\Pi$ descends to a representation $\pi$ of one of the split or non-split symplectic or orthogonal groups $G$ and the preceding two propositions relate the properties of $\Pi$ and $\pi$. Hence I can estimate $N^G_{sd}(\lambda)$ by the number of all cuspidal automorphic representations on $G$ as in Weyl's law. It is not yet known on classical groups, but Donnelly's result [Do] gives an upper bound, which is all I need. The idea of the proof of the lower bound is similar, but the details are more involved, as I need to deal with the full Arthur packets instead of just the generic descent.

In a future work I plan to use similar methods to estimate the number of essentially and conjugate self-dual representations of $GL(N)$, which are functorial lifts from $GSpin$ and unitary groups, respectively.

I have already mentioned some weak results towards the conjectured preservation of depth under functoriality. I plan to study the local descent construction of Jiang-Soudry [JS] (and other explicit constructions of functoriality) in more detail with the hope of proving depth preservation at least in some cases. For classical groups, this requires understanding of what happens to the depth under certain restrictions of representations.

There are other ways which lead to counting local and global representations – for example via the Jacquet-Langlands correspondence or the explicit constructions of supercuspidal representations. For example, Adler [Ad] counted depth zero self-dual supercuspidal representations of $GL_N(F)$. I would like to extend these results to counting supercuspidals on classical groups as well. This is interesting on its own, but I also think that comparing the number of supercuspidals with the number of corresponding Weil-Deligne representations might then yield better results on depth preservation.

## 3. Diophantine equations in weak exponential arithmetics

The question of what strength theories are needed for proving statements such as Fermat's Last Theorem has been of interest for a long time. Notably, Friedman has conjectured that every theorem published in the Annals of Mathematics whose statement involves only finitary mathematical objects (i.e., what logicians call an arithmetical statement) is provable in the so called elementary function arithmetic, which extends usual quantifier free axioms for $0, 1, +, \cdot$, exp, $\leq$ by the scheme of bounded induction. Of course, this conjecture seems to be far out of our reach now.

In my work with Petr Glivický [GK], we study the solvability of Diophantine equations in arithmetics without mathematical induction for multiplication. In such a theory, one obviously can not use the usual inductive definition of the exponential, but we can define the exponential as a function $e$ satisfying a natural set of axioms (such as $e(x, y + z) = e(x, y)e(y, z)$ and $e(e(x, y), z) = e(x, yz)$).

A convenient way of constructing models of arithmetic with such an exponential is to start with a model $\mathcal{B}$ of of $I\Sigma_1$ (which is an extension of Robinson arithmetic by induction for all formulas with only one existential quantifier; we can take e.g. $\mathcal{B} = \mathbb{N}$) and define a substructure $\mathcal{A}$ of $\mathcal{B}$. We classify all exponential functions $e : \mathcal{B} \times \mathcal{A} \to \mathcal{B}$ – they are defined in an explicit way from the usual exponential on $\mathcal{B}$.

We then construct such models (of arithmetic with induction for all formulas in the language $(0, 1, +, \leq)$) $\mathcal{A}$ for which $e : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ and Fermat's Last Theorem does not hold. Namely, $e(a, n) + e(b, n) = e(c, n)$ holds for an unbounded set of quadruples $(a, b, c, n)$.

Surprisingly, we also show that the Catalan Conjecture holds in these models, i.e., the only solution of $e(a, n) - e(b, m) = 1$ with $a, b, n, m > 1$ is $a = m = 3, b = n = 2$ (assuming the ABC Conjecture for $\mathcal{B}$). This gives an interesting separation of the strengths of these two famous Diophantine problems.

It would be exciting to be able to extend these results to much broader classes of Diophantine equations, perhaps even obtaining a classification or hierarchy of their difficulty. Another (apparently hard) problem is to study the exponential functions $e$ in more detail – for example, how do all full exponentials $e : \mathcal{B} \times \mathcal{B} \to \mathcal{B}$ look like?

## References


[Ad] J. D. Adler, *Self-contragradient supercuspidal representations of $GL_n$*, Proc. AMS **125** (1997), 2471 – 2479.

[Ar] J. Arthur, *The Endoscopic Classification of Representations: Orthogonal and Symplectic Groups*, AMS Colloquium Publications **61** 2013, 590 pp.

[BH] M. Bhargava, J. Hanke, *Universal quadratic forms and the 290-theorem*, Invent. Math., to appear.

[BCGK] J. Berg, A. Castillo, R. Grizzard, V. Kala, R. Moy, C. Wang, *Congruences for Ramanujan's f and omega functions via generalized Borcherds products*, Ramanujan J. **35** (2014), 327 – 338.

[BK] V. Blomer, V. Kala, *Number fields without universal n-ary quadratic forms*, Math. Proc. Cambridge Philos. Soc. **159** (2015), 239 – 252.

[CKPS] J. Cogdell, H. Kim, I. Piatetski-Shapiro, F. Shahidi, *Functoriality for the classical groups*, Publ. Math. Inst. Hautes Etudes Sci. **99** (2004), 163 – 233.

[CKR] W. K. Chan, M.-H. Kim, S. Raghavan, *Ternary universal integral quadratic forms*, Japan. J. Math. **22** (1996), 263 – 273.

[DK] A. Dahl, V. Kala, *Distribution of class numbers in continued fraction families of real quadratic fields*, 18 pp., preprint.

[Do] H. Donnelly, *On the cuspidal spectrum for finite volume symmetric spaces*, J. Differential Geom. **17** (1982), 239 - 253.

[GRS] D. Ginzburg, S. Rallis, D. Soudry, *Descent Map from Automorphic Representations of $GL(N)$ to Classical Groups*, World Scientific Publishing Co. Pte. Ltd., 2011, x+339 pp.

[GK] P. Glivický, V. Kala, *Fermat's Last Theorem and Catalan Conjecture in weak exponential arithmetics*, MLQ Math. Log. Q., 17 pp., to appear.

[JKK] J. Ježek, V. Kala, T. Kepka, *Finitely generated algebraic structures with various divisibility conditions*, Forum Math. **24** (2012), 379 – 397.

[JS] D. Jiang, D. Soudry, *On the Local Descent from $GL(n)$ to Classical Groups*, Amer. J. Math. **134** (2012), 767 – 772.

[Ka] V. Kala, *Universal quadratic forms and elements of small norm in real quadratic fields*, Bull. Aust. Math. Soc. **94** (2016), 7 – 14.

[Ka2] V. Kala, *Weak Weyl's Law for self-dual automorphic representations of $GL_n(\mathbb{A}_{\mathbb{Q}})$*, 24 pp., submitted.

[Ka3] V. Kala, *Lattice-ordered abelian groups finitely generated as semirings*, J. Commut. Algebra, 16 pp., to appear.

[KM] V. Kala, P. Maga, *On orthogonal matrices with prescribed Smith normal form*, in preparation.

[Ki1] B. M. Kim, *Finiteness of real quadratic fields which admit positive integral diagonal septenary universal forms*, Manuscr. Math. **99** (1999), 181 – 184.

[Ki2] B. M. Kim, *Universal octonary diagonal forms over some real quadratic fields*, Commentarii Math. Helv. **75** (2000), 410 – 414.

[Le] E. Leichtnam, *A classification of the commutative Banach perfect semi-fields of characteristic 1. Applications*, arxiv:1606.00328.

[Mu] W. Müller, *Weyl's law for the cuspidal spectrum of $SL_n$*, Ann. of Math. (2) **165** (2007), 275 - 333.

[Ro] D. Rohrlich, *Self-dual Artin representations*, in *Automorphic Representation and L-functions*, Tata Inst. Fundam. Res. Stud. Math. **22** (2013), 455 – 499.

[Si] C. L. Siegel, *Sums of $m$-th powers of algebraic integers*, Ann. of Math. (2) **46** (1945), 313 – 339.