# 1 Summary

My research is in the general area of *number theory*. I use a wide variety of methods across number theory including sieve methods, the determinant method of Heath-Brown and Salberger, arithmetic invariant theory, and geometry of numbers. More recently, I have begun to investigate problems in arithmetic geometry, inspired by the recent breakthrough of B. Lawrence and A. Venkatesh [42].

For my thesis I worked largely on extending the $p$-adic determinant method, a novel new method in diophantine geometry introduced by Heath-Brown in [32] into the setting of *weighted projective varieties*, and with this extension I was able to give improvements for power-free values of binary forms [1]. This improvement of the determinant method uses a significant number of tools from algebraic geometry.

Subsequently, I have worked on problems involving representation of integers by various polynomials. In particular, together with C.L. Stewart, we solved a long-standing conjecture on the density of integers represented by a binary form $F$ of degree at least three [8]. Our work in this area uses tools from both algebraic and analytic number theory.

On the more algebraic side, I have worked on counting problems for $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary forms which has applications in counting certain kinds of number fields. This work is with C. Tsang (see [10] [11]). The influence behind our work in this area is the seminal work of Bhargava and Shankar [17] and Melanie Wood [53] in arithmetic invariant theory and geometry of numbers. However, significant technical innovation and new ideas are needed to achieve progress in our papers. More recently, I have done work on the negative Pell equations and generalizations to other roots of unity with Erick Knight.

# References

## Articles by me

[1] *Power-free values of binary forms and the global determinant method*, International Mathematics Research Notices, Issue 16 Volume 2017 (2017), 5078-5135.

[2] *On binary cubic and quartic forms*, arXiv:1610.09208 [math.NT], to appear in Journal de Thorie des Nombres de Bordeaux.

[3] *Square-free values of decomposable forms*, Canadian Journal of Mathematics **70** (2018), 1390-1415.

[4] *Binary quartic forms with vanishing $J$-invariant*, arXiv:1712.09091 [math.NT], submitted to International Mathematics Research Notices (28 pages).

[5] *On monic abelian cubics*, arXiv:1906.08625 [math.NT], submitted to Compositio Mathematica (13 pages).

## Co-authored articles

[6] K. Lapkova, S. Y. Xiao, *The density of $k$-free values of polynomials*, Mathematika (4) **65** (2019), 1038-1050.

[7] P. C. Lam, D. Schindler, S. Y. Xiao, *On prime values of binary quadratic forms with a thin variable*, arXiv:1809.10755 [math.NT], submitted to Journal of the London Mathematical Society (26 pages).

[8] C. L. Stewart, S. Y. Xiao, *On the representation of integers by binary forms*, Mathematische Annalen **375** (2019), 133-163.

[9] C. L. Stewart, S. Y. Xiao, *On the representation of $k$-free integers by binary forms*, arXiv:1612.00487 [math.NT], to appear in Revista Matematica Iberoamericana.

[10] C. Tsang, S. Y. Xiao, *Binary quartic forms with bounded invariants and small Galois groups*, arXiv:1702.07407 [math.NT], to appear in Pacific Journal of Mathematics.

[11] C. Tsang, S. Y. Xiao, *The number of quartic D4-fields with monogenic cubic resolvent ordered by conductor*, arXiv:1712.08552 [math.NT], submitted to Transactions of the American Mathematical Society (28 pages).

[12] S. Y. Xiao, S. Yamagishi, *Zeroes of polynomials in many variables with prime inputs*, arXiv:1512.01258 [math.NT], to appear in Canadian Journal of Mathematics.

## Preprints

[13] E. Knight, S. Y. Xiao, *On the $\zeta_3$-Pell equation*

[14] B. Nasserden, S. Y. Xiao, *Uniformity of period mappings and solutions to the $S$-unit equation*

## 2 The global determinant method

In diophantine geometry, one reduces the problem of counting solutions to polynomial equations to one about the *density* of rational or integral points on an algebraic variety. For an algebraic projective variety $X$ defined over $\mathbb{Q}$, each rational point is represented by a *primitive* integral point. Define

$$N_X(B) = \#\{\mathbf{x} \in X \cap \mathbb{Z}^n : |x_i| \leq B \text{ for } 1 \leq i \leq n, \gcd(x_1, \cdots, x_n) = 1\}. \quad (1)$$

Let $d$ be the degree of $X$. When $d$ is very small compared to $n$, the classical Hardy-Littlewood circle method gives that for any $X$ there exists a positive number $c(X)$ such that

$$N_X(B) \sim c(X)B^{n-d}. \quad (2)$$

Indeed, for smooth projective varieties $X$ which arise as complete intersections of forms of equal degree, a seminal theorem of Birch shows that (2) holds whenever $n > (d+1)2^d$. For $d = 3$, it is known by work of Davenport and Heath-Brown that (2) holds whenever $n \geq 10$ and that there exist examples where (2) fails for $n < 10$. For a long time, the behaviour of $N_X(B)$ for $d > n$ remained a complete mystery.

In 2002 [32], D. R. Heath-Brown introduced a novel new method which generalized the so-called *determinant method* of Bombieri-Pila [19]. This new version, which uses congruences relations modulo primes rather than distances in Euclidean space, was later dubbed the $p$-adic determinant method. Unlike the original Bombieri-Pila version, Heath-Brown's $p$-adic determinant method is applicable to varieties of arbitrarily large dimension (in [32] Heath-Brown only developed the method for projective hypersurfaces; the generalization to arbitrary projective varieties was achieved in a later paper by Browning, Heath-Brown, and Salberger [20]). In particular, Heath-Brown's determinant method, subsequently refined by Salberger [46], allows one to deduce the bound

$$N_X(B) = O_{d,n,\varepsilon}\left(B^{n-2+\varepsilon}\right)$$

for any projective variety $X$ of degree $d \geq 4$ which does not contain a hyperplane of dimension $\dim X$. Moreover, the implied constant only depends on $d, n, \varepsilon$, and so is *uniform* in the coefficients of the polynomials defining $X$. This fact can be extremely important in applications.

The determinant method has been applied to prove several noteworthy results in diophantine geometry. Notably, it has been applied by Heath-Brown in [32] to show that for any projective surface $X$ and $U$ the Zariski open subset of $X$ consisting of the complement of the lines contained in $X$, that the number of rational points of height at most $B$ in $U(\mathbb{Q})$ is at most $O_{d,\varepsilon}\left(B^{52/27+\varepsilon}\right)$. This has applications to the study of the density of integers represented by binary forms; see the next section.

One other major application of the determinant method is the study of $k$-free values of polynomials. In [33], Heath-Brown devised a version of the $p$-adic determinant method applicable to affine varieties, and used it to prove that a polynomial $f(x)$ of degree $d$ takes on the expected density of $k$-free values provided that $k \geq (3d+2)/4$.

Heath-Brown's formulation of the $p$-adic determinant method uses one prime at a time. This turns out to be relatively inefficient, and usually requires one to impose more stringent conditions on the degree of the variety to obtain acceptable bounds. In [46], P. Salberger refined Heath-Brown's method and obtained what is now called the *global* determinant method. Salberger had used the global

determinant method to count points on Fermat hypersurfaces, and Walsh used it to show that for any projective curve $\mathcal{C}$ of degree $d$ embedded in $\mathbb{P}^n$, the number of rational points on $\mathcal{C}$ of height $B$ can be uniformly bounded by $O_{d,n}\left(B^{1/d}\right)$ [52].

In [1], I obtained a generalization of Salberger's global determinant method, proved in the setting of projective spaces, to the setting of *weighted* projective space. An application of this result is an improvement to estimating $k$-free values of binary forms; see Section 4.

More recently, I have also combined Heath-Brown's affine determinant method in [33] and Salberger's global determinant method to obtain the density of $k$-free values of polynomials in any number of variables satisfying the necessary conditions. This is joint work with K. Lapkova [6].

# 3 Representation of integers by binary forms

Perhaps the nicest class of binary polynomials are the *binary forms*, or homogeneous polynomials in two variables. They share a fundamental property with polynomials in a single variable, namely that any binary form splits into linear forms over an algebraically closed field. A natural question to ask is *which integers $h$ can be represented by a binary form*? For a binary form $F$ of degree $d$, we put

$$\mathcal{R}_F(Z) = \{h \in \mathbb{Z} : |h| \leq Z, h \text{ is representable by } F\}. \tag{3}$$

for the set of *representable integers* of size at most $Z$. We wish to understand the cardinality of this set, $R_F(Z) = \#\mathcal{R}_F(Z)$.

This problem has attracted the attention of many mathematicians over the past century. Landau proved an asymptotic formula for $R_F(Z)$ when $F$ is a quadratic form, but believed that this case is quite exceptional. Mahler proved in [43] that $R_F(Z)$ is bounded by $A_F Z^{2/d}$, where $A_F$ is the area of the region $\{(x, y) \in \mathbb{R}^2 : |F(x, y)| \leq 1\}$. Erdős and Mahler gave a lower bound of the same order of magnitude in [26]. Hooley gave the first asymptotic formula for a form of degree exceeding two in [35], namely irreducible cubic forms with non-square discriminant, and over 33 years obtained the asymptotic formula for quartic forms of the shape $Ax^4 + Bx^2y^2 + Cy^4$ and the remaining irreducible binary cubic

forms in [36] and [38]. Many authors have worked on diagonal forms of the shape $Ax^d + By^d$; see [8] for a summary.

In [8], C. L. Stewart and I essentially settled this problem. Recall that $\mathrm{GL}_2$ acts on a binary form $F$ via substitution. Put $\mathrm{Aut}(F)$ for the group of $\mathrm{GL}_2(\mathbb{Q})$-automorphisms of $F$ under this action. We then proved the following:

**Theorem 3.1** (Stewart, Xiao)**.** *Let $F$ be a binary form of degree $d \geq 3$, integer coefficients, and non-zero discriminant. Then there exists a positive number $C_F$ and a positive number $\beta_d < 2/d$, depending only on the degree $d$, such that for any $\varepsilon > 0$ the asymptotic formula*

$$R_F(Z) = C_F Z^{\frac{2}{d}} + O_{F,\varepsilon}\left(Z^{\beta_d+\varepsilon}\right) \tag{4}$$

*holds. Moreover, the constant $C_F$ can be expressed as $W_F A_F$, where $W_F$ is a positive rational number that can be given explicitly in terms of* $\mathrm{Aut}(F)$*.*

Our theorem builds on an earlier result of Heath-Brown in [32], which states that all but a negligible number of representable integers in $[-Z, Z]$ are *essentially represented*. We say that a representable integer $h$ is essentially represented if whenever $F(x, y) = F(u, v) = h$, there exists a $\mathrm{GL}_2(\mathbb{Q})$-automorphism of $F$ which sends $(x, y)$ to $(u, v)$. Heath-Brown proved this using the $p$-adic determinant method which he introduced in [32]. The exponent $\beta_d$ uses the global determinant method of Salberger [46] [47].

While we proved the existence of the asymptotic formula (4) for all binary forms $F$ with non-zero discriminant, there is still the issue of determining the automorphism group $\mathrm{Aut}(F)$. While $\mathrm{Aut}(F)$ is trivial, i.e., equal to $\{I_{2\times 2}\}$ for odd degrees and $\{\pm I_{2\times 2}\}$ for even degrees for 100% of binary forms of any given degree (sorted by height of the coefficients say), in which case $W_F = 1$, it is still an interesting question to determine $\mathrm{Aut}(F)$ in general. Indeed, Hooley had accomplished exactly this for the cases he dealt with in [35], [36], and [37]. I finished the work of Hooley by determining $\mathrm{Aut}\, F$ explicitly for all binary cubic and quartic forms in [2]. I proved the following:

**Theorem 3.2.** *Let $F$ be a binary cubic or quartic form with integer coefficients and non-zero discriminant. Then* $\mathrm{Aut}(F)$ *can be given explicitly in terms of certain quadratic covariants of $F$. Moreover, whenever $T \neq \pm I_{2\times 2} \in \mathrm{Aut}(F)$, the corresponding quadratic covariant is defined over $\mathbb{Q}$.*

For the cubic case, these quadratic covariants were given by G. Julia, and in the quartic case, they were discovered by Cremona in [24].

# 4 $k$-free values of polynomials

Aside from being interested in which integers can be represented by a given polynomial, there is also significant interest in which special integers, such as the primes, can be represented by the integers. Dirichlet famously proved that each linear polynomial $ax+b$ with $\gcd(a,b)=1$ represents infinitely many primes, even giving the density of primes which can be represented as such. Siegel famously proved that any polynomial $f$ with integer coefficients, non-zero discriminant, and degree at least three can only represent finitely many squares (in other words, the hyperelliptic curve $y^2=f(x)$ contains only finitely many integral points, a prelude to Faltings' theorem).

## 4.1 $k$-free values of binary forms

In my work, I have studied the problem of representing $k$-free values by binary forms. An integer $n$ is said to be $k$-free if it is indivisible by the $k$-th power of any prime number.

There are primarily two types of results in the literature. The first type, initiated by Granville in [30] and leading to the work of Poonen [45] and Murty-Pasten [44], establishes that polynomials take on infinitely many square-free values (and hence $k$-free values for any $k \geq 2$) assuming the *abc*-conjecture. The second type attempts to obtain results for $k$-free values represented by polynomials unconditionally. There is a vast literature of this latter type; see [1] for a detailed summary.

The first contribution I made to this subject is the following theorem for binary forms:

**Theorem 4.1.** *Let $F$ be a binary form of degree $n \geq 3$, integer coefficients, and non-zero discriminant. Let $k \geq 2$ be a positive integer. Suppose that for any prime $p$ there exist integers $(m_p, n_p)$ such that $p^k \nmid F(m_p, n_p)$. Let $d$ denote the degree of*

*the largest irreducible factor of $F$. For a positive number $B$, put*

$$N_{F,k}(B) = \#\{(x,y) \in \mathbb{Z}^2 : |x|, |y| \leq B, F(x,y) \text{ is } k\text{-free}\}.$$

*Then there exists a positive number $C_{F,k}$ for which the asymptotic formula*

$$N_{F,k}(B) \sim C_{F,k} B^2 \tag{5}$$

*holds, provided that*

$$k > \min\left\{\frac{7d}{18}, \left\lceil \frac{d}{2} \right\rceil - 2\right\}. \tag{6}$$

The positive number $C_{F,k}$ in Theorem 4.1 is a product of local factors.

Analogous to the representation of integers case, one might wonder how many $k$-free integers in an interval can be represented by a given form. This question is somewhat more difficult to answer. Indeed, previously we did not even have an analogue to Mahler's theorem for $k$-free values; Theorem 4.1 being a strictly weaker form as it only counts pairs in a bounded box rather than in a non-compact region as demanded by Mahler's theorem. Nevertheless, various authors in the literature have been able to prove the analogue of Erdős and Mahler's theorem for $k$-free values, beginning with Gouvêa and Mazur [29] and then by Stewart and Top [50]. I extended Stewart and Top's theorem in [1]:

**Theorem 4.2.** *Let $F$ be a binary form as in Theorem 4.1. For a positive number $Z$ and a positive integer $k \geq 2$, put*

$$R_{F,k}(Z) = \#\{h \in \mathbb{Z} : |h| \leq Z, h \text{ is } k\text{-free}, \exists (x,y) \in \mathbb{Z}^2 \text{ s.t. } F(x,y) = h\}.$$

*Suppose that $k$ satisfies (6). Then there exist positive numbers $C_1, C_2$ such that*

$$R_{F,k}(Z) > C_1 Z^{\frac{2}{n}}$$

*whenever $Z > C_2$.*

By combining the results in [1] and [8], Stewart and I managed to prove the following theorems in [9]:

**Theorem 4.3** (Stewart, Xiao)**.** *Let $F$ be a binary form as in Theorem 4.1, and let $k \geq 2$ be a positive integer satisfying (6). Then there exists a positive number $C'_{F,k}$ such that the asymptotic formula*

$$R_{F,k}(Z) \sim C'_{F,k} Z^{\frac{2}{n}}$$

*holds.*

**Theorem 4.4** (Stewart, Xiao)**.** *Let $F$ be a binary form as in Theorem 4.1, and let $k \geq 2$ be a positive integer satisfying (6). For a positive number $Z$ put*

$$N_{F,k}(Z) = \#\{(x,y) \in \mathbb{Z}^2 : 0 < |F(x,y)| \leq Z, F(x,y) \text{ is } k\text{-free}\}.$$

*Then there exists a positive number $C''_{F,k}$ such that the asymptotic relation*

$$N_{F,k}(Z) \sim C''_{F,k} Z^{\frac{2}{n}}$$

*holds.*

The numbers $C'_{F,k}$ and $C''_{F,k}$ are again related to automorphisms of the form; one has to be careful about contributions of the automorphism group $\operatorname{Aut} F$ of $F$.

## 4.2 Square-free values of decomposable forms

The most sought after results in this subject are of course results concerning square-free values. Without assuming the *abc*-conjecture, results are relatively few and far in between. The known cases for polynomials which take on infinitely many square-free values are as follows:

1. Single variable polynomials whose largest irreducible factor does not have degree exceeding 3, due to Hooley [35];
2. Binary forms whose largest irreducible factor does not have degree exceeding 6, due to Greaves [31];
3. Binary polynomials which splits into linear factors over $\overline{\mathbb{Q}}$ and whose largest irreducible factor has degree not exceeding 6, due to Hooley [37];
4. Discriminants of binary cubic forms, pairs of ternary quadratics, and quadruples of skew symmetric matrices, due to Bhargava [16]; and
5. Discriminants of polynomials in a single variable, due to Bhargava, Shankar, and Wang [18].

We extended the unconditional knowledge of square-free values of polynomials by extending the work of Greaves and Hooley to *decomposable forms*. In some sense, the setting of decomposable forms is the most naturalization for the results of Greaves and Hooley. A homogeneous polynomial $f(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n]$ is said to be a decomposable form if it splits over $\overline{\mathbb{Q}}$. We proved the following in [3]:

**Theorem 4.5.** *Let $F$ be a decomposable form in $n$ variables and degree $r > n$. Let $d$ be the degree of the largest irreducible factor of $F$. Let $k \geq 2$ be an integer, and suppose that for all primes $p$ there exists an $n$-tuple of integers $(m_1, \cdots, m_n)$ such that $p^k \nmid F(m_1, \cdots, m_n)$. For a positive number $B$ put*

$$N_{F,k}(B) = \#\{(x_1, \cdots, x_n) \in \mathbb{Z}^n : |x_i| \leq B \text{ for } i = 1, \cdots, n, F(x_1, \cdots, x_n) \text{ is } k\text{-free}\}.$$

*Then there exists a positive number $C_{F,k}$ for which the asymptotic formula*

$$N_{F,k}(B) \sim C_{F,k} B^n \tag{7}$$

*holds whenever $d \leq 2n + 2$.*

Observe that when $n = 2$, this recovers Greaves's theorem in [31].

Although this theorem looks similar to Theorem 4.1, the proof is materially different. Indeed, the determinant method is highly sensitive to dimension, and in larger dimensions do not yield satisfactory bounds. The proof of Theorem 4.5 uses Greaves's geometry of numbers argument as well as an adaptation of Hooley's use of the Selberg sieve in [36] and [37].

### 4.3 $k$-free values of polynomials in many variables

In joint work with K. Lapkova [6], we obtain for polynomials in any number of variables satisfying the necessary conditions the analogous asymptotic formula (7). This involves using the global version of Heath-Brown's affine determinant method.

## 5 Diophantine problems with prime coordinates

Among the most interesting problems in number theory are questions asking whether equations can be solved in the prime numbers. Surprisingly little is known in this area. For example, even the simple linear equation $x - y = 2$ is not known to have infinitely many solutions in prime variables $x$ and $y$; and it is only due to the recent seminal work of Yitang Zhang and James Maynard that we are able to say that there exists some natural number $N$ (indeed, infinitely many)

such that $x - y = 2N$ has infinitely many solutions in primes.

In [23], Cook and Magyar broke new ground by showing that with systems of polynomial equations in many variables (relative to the degrees of the equations), one can always ensure that solutions exist with all inputs being prime provided that the number of variables is sufficiently large and that the system is sufficiently non-singular. The device they used to measure non-singularity is something called the Birch singular locus. This device is essential for analytic arguments but is regarded as inessential from a number theoretic point of view, so it is of interest to remove such strong hypotheses.

W. M. Schmidt introduced an invariant of homogeneous polynomials, now called Schmidt's $h$-invariant, which measures how close a homogeneous polynomial is to be reducible. Indeed, $h(F)$ of a homogeneous polynomial $F$ is equal to the smallest positive integer $r$ such that $F$ can be written as the sum of $r$ reducible forms. We then see that $h(F) = 1$ if and only if $F$ is reducible. One expects that Cook and Magyar's results should hold with the Birch singular locus replaced by the $h$-invariant.

In [12], S. Yamagishi and I made progress towards this problem. We introduced a slightly more restrictive invariant $h^*(F)$, which is the smallest positive integer $r$ such that $F$ can be written as a sum of $r$ reducible forms, each being divisible by a linear form. Clearly, $h(F) \leq h^*(F)$. We showed that assuming $h^*(F)$ is sufficiently large, then the conclusion of Cook and Magyar's work still holds. We then note that if $\deg F \leq 3$, then $h(F) = h^*(F)$ so that Cook and Magyar's results hold for quadratic and cubic forms in many variables provided only that the Schmidt invariant is large.

## 5.1 Primes represented by binary quadratic forms with a prime input

In forthcoming work with D. Schindler, we improve upon a theorem of Fouvry and Iwaniec by showing that positive definite binary quadratic forms $f$ capture their primes, even with one coordinate restricted to be prime. This requires a non-trivial treatment of the complication caused by non-trivial class groups corresponding to general quadratic forms.

# 6 Counting algebraic objects

In 2010 (published in 2015), Bhargava and Shankar developed a radically new method to attack the problem which allowed them to prove, *unconditionally* that the average rank of elliptic curves is bounded. They did so by counting $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary quartic forms.

Inspired by the work of Bhargava and Shankar and observing that my work in [2] can be used to parametrize binary quartic forms with small Galois group (that is, irreducible quartic forms whose Galois groups are not $S_4$ or $A_4$), C. S. Tsang and I obtained parametrization and counting theorems for binary quartic forms with small Galois groups in [10]. Let $V_{\mathbb{R}}$ denote the 5-dimensional real vector space of binary quartic forms, In [10], we showed that each $\mathrm{GL}_2(\mathbb{Z})$-class of integral binary quartic forms with small Galois group has a representative in a countable family of 3-dimensional subspaces $V_{f,\mathbb{R}}$ of $V_{\mathbb{R}}$, indexed by $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of binary *quadratic* forms. Moreover, these subspaces are more or less distinct in the sense that if $f, g$ are $\mathrm{GL}_2(\mathbb{Z})$ distinct binary quadratic forms, then the integral elements in $V_{f,\mathbb{R}}, V_{g,\mathbb{R}}$ are mostly $\mathrm{GL}_2(\mathbb{Z})$-distinct.

The deficit of our work in [10] is that it does not allow one to count *all* $\mathrm{GL}_2(\mathbb{Z})$-classes of binary quartic forms with small Galois group, but only one family indexed by a given $\mathrm{GL}_2(\mathbb{Z})$-class of binary quadratic form at a time. This, for example, does not allow one to prove what Bhargava and Shankar proved in [17], namely to compute the average size of the 2-Selmer group of elliptic curves when sorted by height (it turns out in the case of curves with small Galois group, the size of the 2-Selmer group is unbounded on average). However, we have been able to apply our work in [10] in studying a different type of algebraic object.

## 6.1 Quartic fields with monogenic cubic resolvent and small Galois group

The notion of "small Galois group" applies equally well to *quartic orders*. In her thesis, Wood proved that $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of integral binary quartic forms correspond exactly to a pair $(Q, C)$, where $Q$ is a quartic order and $C$ is a monogenic cubic resolvent ring of $Q$. She also gave a parametrization of triples $(Q, C, T)$, where $Q$ is a quartic order, $C$ a cubic resolvent ring of $Q$, and $T$ the

biggest quadratic subalgebra of $Q$ in terms of equivalence classes of certain pairs of ternary quadratic forms, refining the work of Bhargava in [15]. When $Q$ is an order in a quartic field, this case corresponds exactly to quartic orders with small Galois group. Combining these ideas, and using a novel consequence of my paper [2] and our joint work with Tsang [10], we were able to parametrize maximal quartic orders with monogenic cubic resolvent and small Galois group.

**Theorem 6.1** (Tsang, Xiao)**.** *Let $Q$ be a quartic order with small Galois group. For a binary quartic form $F$, let $R_F$ denote the quartic order corresponding to the $\mathrm{GL}_2(\mathbb{Z})$-class of $F$ via Wood's correspondence. If $Q$ is a maximal order, then there exists an $F$ lying in one of the following three families for which $Q = R_F$:*

*(a)* $W^{(1)} = \{Ax^4 + Bx^2y^2 + Cy^4 : A, B, C \in \mathbb{Z}\}$*;*

*(b)* $W^{(2)} = \{Ax^4 + Bx^3y + Cx^2y^2 - Bxy^3 + Ay^4 : A, B, C \in \mathbb{Z}\}$*; and*

*(c)* $W^{(3)} = \{Ax^4 + Bx^3y + Cx^2y^2 + Bxy^3 + Ay^4 : A, B, C \in \mathbb{Z}\}$.

Using this theorem, one can then use our results in [10] to count maximal quartic orders with monogenic cubic resolvent and small Galois group, which then corresponds to quartic fields. The difficulty that needs to be surmounted is how to count the quartic forms in the families $W^{(i)}$ *by discriminant*, which in the case of all binary quartic forms is a very difficult problem, requiring a hypothesis seemingly stronger than even the *abc*-conjecture. However in our case this difficult problem can be overcome because the discriminant polynomial for quartic forms in each of the families $W^{(i)}$ factors, and this makes the problem approachable. Theorem 6.1 and the corresponding counting theorem will appear in [11].

## 6.2 Binary quartic forms with vanishing $J$-invariant

Bhargava's work on enumerating quartic and quintic fields, Bhargava and Shankar's work on counting binary quartic forms, ternary cubic forms, and objects associated to higher $n$-Selmer elements, as well as the work of Bhargava, Shankar, and Tsimerman on counting binary cubic forms represent an exciting new chapter in geometry of numbers. However, despite the major advance that they represent, the method of Bhargava currently has a fundamental limitation: it requires that the action of a reductive group on a vector space give rise to a ring of polynomial invariants which can be generated by algebraically independent elements. Such a pair $(G, V)$, with $G$ a reductive group and $V$ a vector space

on which $G$ acts, is called a co-regular space. In general, in order to generalize Bhargava's methods, one has to solve the so-called *subvariety problem*, which amounts to being able to treat the situation of a pair $(G, \mathcal{V})$, where $\mathcal{V} \subset V$ is a proper subvariety.

Perhaps the simplest cases are the two non-trivial (and interesting) subvarieties of $V_4$, the space of binary quartic forms, given by the vanishing of the $I$ and $J$ invariants respectively. These two varieties are respectively a quadric $Q_4$ and a cubic threefold $K_4$ which are invariant under the action of $\mathrm{GL}_2(\mathbb{R})$ on $V_4$. In his thesis, S. Ruth gave an interesting idea of applying Heath-Brown's circle method to count $\mathrm{GL}_2(\mathbb{Z})$-orbits in $Q_4$. Recently in [4], I managed to enumerate the number of totally real $\mathrm{GL}_2(\mathbb{Z})$-orbits inside $K_4$. There is a richness of structure that can be exploited that should enable one to count all integral orbits inside $K_4$; we hope to pursue this in the near future.

## 6.3 Monic abelian cubics

Perhaps one of the oldest results in the area of arithmetic statistics, and likely the result that kicked off the subject area to begin with, is the so-called Hilbert irreducibility theorem: it asserts that, when consider the set of *monic* polynomials of degree $n \geq 2$

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n, a_i \in \mathbb{Z}, \tag{8}$$

and ordering the polynomials by the box height $H(f) = \max\{|a_1|, \cdots, |a_n|\}$, that a proportion tending to 100% of degree $n$ integral monic polynomials will be irreducible and have Galois group isomorphic to the symmetric group $S_n$. By looking at polynomials of the shape (8) with $a_n = 0$, we see that there are $\gg X^{n-1}$ polynomials $f$ with $H(f) \leq X$ which are reducible.

Put $N_{S_n}^{(n)}(X)$ for the number of degree $n$ polynomials $f$ given by (8) which are irreducible and have Galois group isomorphic to $S_n$ with $H(f) \leq X$, and let $N^{(n)}(X)$ denote the total number of such polynomials $f$ with $H(f) \leq X$. Van der Waerden had conjectured the precise asymptotic formula

$$\left| N^{(n)}(X) - N_{S_n}^{(n)}(X) \right| = O\left(X^{n-1}\right). \tag{9}$$

In other words, irreducible polynomials with Galois group strictly smaller than $S_n$ are at most as rare as reducible polynomials.

One can formulate the question in a more precise fashion. Let $G < S_n$ be a transitive subgroup, and let $N_G^{(n)}(X)$ be the number of degree $n$ polynomials $f$ satisfying (8) with Galois group isomorphic to $G$, and $H(f) \leq X$. We wish to establish an asymptotic bound of the form

$$N_G^{(n)}(X) = O\left(X^{n-\delta_{G,n}}\right) \tag{10}$$

for all such groups $G$. Van der Waerden's conjecture is then the assertion that $\delta_{G,n} \geq 1$ for all transitive, proper $G < S_n$.

In [5], I established (10) for the case $n = 3$ and $G = C_3$, which is the first non-trivial case, with the value $\delta_{C_3,3} = 5/3$. Numerical evidence compiled by S. Chow and R. Dietmann (private communication) seems to indicate that this bound is sharp, but we have not been able to find sufficiently many such polynomials to confirm a lower bound of the same order of magnitude.

As a surprising consequence of our investigations, we proved the following theorem about elliptic curves:

**Theorem 6.2.** *Let $E/\mathbb{Q}$ be an elliptic curve which is semi-stable over $\mathbb{Q}$ and such that $K = \mathbb{Q}(E[2])$ is a cyclic cubic field, where $E[2]$ denotes the subgroup of $E(\overline{\mathbb{Q}})$ consisting of points of order 2. Then $K = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, where $\zeta_9$ is a primitive 9-th root of unity.*

This theorem gives the possibility that one can investigate the average size of the 2-Selmer group of semi-stable curves with cyclic cubic 2-torsion, much like in the paper of G. Yu [54] who treated the case when all of the 2-torsion points are defined over $\mathbb{Q}$.

# 7 Pellian equations

A classical equation with its origins tracing back to ancient Greece, and in the modern era of mathematics has its name misattributed by Euler to John Pell, is the equation

$$x^2 - dy^2 = 1, d \in \mathbb{N}, d \text{ is square-free.} \tag{11}$$

It is now well-known that the Pell equation is always soluble in the integers and indeed has infinitely many solutions, and is the first case of Dirichlet's unit theorem. However the so-called *negative Pell equation*

$$x^2 - dy^2 = -1, d \in \mathbb{N}, d \text{ is square-free} \tag{12}$$

is much more mysterious. It is a simple exercise to show that for most natural numbers $d \leq X$, in the sense of natural density, the equation (12) has no solution in the integers. Determining the exact density of those $d \leq X$ where (12) has a solution remains one of the most difficult problems in mathematics. Fouvry and Klüners made substantial progress on this problem in [28].

In joint work with Erick Knight, we are generalizing the result of Fouvry and Klüners to the case of the so-called $\zeta_3$-Pell equation. Put $K = \mathbb{Q}(\zeta_3)$, where $\zeta_3$ is a non-trivial cubic root of unity. We then ask which cubic extensions $L/K$ with $L = K(\sqrt[3]{\alpha})$ and $\alpha$ an integer in $K$ does there exist a solution to the equation

$$N_{L/K}(x) = \zeta_3, \tag{13}$$

where $N_{L/K}(\cdot)$ is the norm of $L$ over $K$. We have shown that the story plays out somewhat similarly, in that there exists an analogue to Gauss's genus theory, the existence of governing fields for higher order torsion, and equidistribution of cubic symbols. This is also related to recent seminal work of Alexander Smith [48].

# 8 Proofs of Mordell's conjecture, and the uniform boundedness conjecture

In 1922, L. Mordell famously conjectured the following elegant statement regarding the behaviour of rational points on algebraic curves:

**Conjecture 8.1** (Mordell's conjecture)**.** *Let $K$ be a number field, $g \geq 2$ an integer, and $X/K$ an algebraic curve defined over $K$ having genus $g$. Then the set of $K$-rational points $X(K)$ of $X$ is finite.*

The profoundness of Mordell's conjecture lies in its simple elegance: a purely geometrical invariant, the genus, is enough to determine diophantine finiteness.

In 1983, Faltings famously proved Mordell's conjecture, building on earlier work of Parshin. In doing so he also solved two other famous mathematical problems, namely Shafarevich's conjecture on the finiteness of isomorphism classes of curves having genus $g \geq 2$ having good reduction outside of a finite set $S$ of primes, and Tate's conjecture for abelian varieties defined over number fields.

Faltings' proof had the deficit that it does not allow one to effectively determine the set of rational points $X(K)$. This is still a difficult open problem in general. However, Faltings' argument does in fact give an upper bound for the cardinality of $X(K)$, which in general depends quite badly on $X$.

A refinement of Faltings' theorem is the following:

**Conjecture 8.2** (Uniform boundedness conjecture)**.** *Let $K$ be a number field and $g \geq 2$ a positive integer. Then there exists a positive number $N(K, g)$ such that for any curve $X$ defined over $K$ having genus $g \geq 2$, we have $|X(K)| \leq N(K, g)$.*

It is a surprising result of Caporaso, Harris, and Mazur [22] that assuming the Bombieri-Lang conjecture, which simply asserts that for varieties $Z$ of general type defined over a number field $K$, the set $Z(K)$ of $K$-rational points is not Zariski dense, that Conjecture 8.2 holds. In groundbreaking work, Stoll showed in [51] that Conjecture 8.2 holds for hyperelliptic curves over $\mathbb{Q}$ satisfying $r \leq g - 3$, where $r$ is the (rational) Mordell-Weil rank. Refining Stoll's argument, Katz, Rabinoff, and Zuerick-Brown showed in [41] that Conjecture 8.2 holds for arbitrary algebraic curves $X$ over any number field $K$ with $r \leq g - 3$, where $r$ is now the $K$-rational Mordell-Weil rank of $X$.

More recently, Lawrence and Venkatesh [42] introduced a significant refinement of Parshin's construction. Indeed, they showed that Mordell's conjecture follows from a statement about finiteness of fibres of a certain $p$-adic period mapping. In doing so, they have eliminated the necessity to consider Faltings' height in the proof of Mordell, relying only on a statement about finiteness of global Galois representations of fixed dimension having good reduction outside a finite set of primes (this result is also due to Faltings and was needed in Faltings' original proof).

In a recent preprint, Brett Nasserden and I showed that the approach of Lawrence and Venkatesh essentially gives uniform bounds for the number of rational points,

up to the dependency on the number of relevant global Galois representations. We also give the example of elliptic curves over $\mathbb{Q}$ to suggest that perhaps one can expect the number of such Galois representations to be uniformly bounded. Finally, our argument does unconditionally give uniform bounds for $S$-unit equations, recovering an earlier result of J-H. Evertse [27].

# 9 Future work

In an ongoing project with Erick Knight, we are looking at extending Alex Smith's ideas given in [48] to apply to the negative Pell equation. The key difficulty appears to be a subtle issue of Smith's machinery enabling one to construct generalized governing fields which controls the distribution of $2^k$-ranks of class groups, where his machinery appears to require an assumption about the genericness of discriminants, which does not apply to the discriminants for which the negative Pell equation is potentially soluble. We hope to refine the construction and perhaps develop more algebraic tools to overcome this issue.

I am continuing to investigate the uniform boundedness conjecture, even in the special case of twist families. One promising approach is to attempt to unite the approach of Lawrence and Venkatesh in [42] with non-abelian philosophy espoused by Minhyong Kim.

# Other references

[15] M. Bhargava, *Higher composition laws III : The parametrization of quartic rings*, Annals of Mathematics, **159** (2004), 1329-1360.

[16] M. Bhargava, *The geometric sieve and the density of squarefree values of invariant polynomials*, arXiv:1402.0031 [math.NT].

[17] M. Bhargava, A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Annals of Mathematics **181** (2015), 191-242.

[18] M. Bhargava, A. Shankar, X. Wang, *Squarefree values of polynomial discriminants I*, arXiv:1611.09806 [math.NT].

[19] E. Bombieri, J. Pila, *The number of integral points on arcs and ovals*, Duke Mathematical Journal, (2) **59** (1989), 337-357.

[20] T. D. Browning, D. R. Heath-Brown, P. Salberger, *Counting rational points on algebraic varieties*, Duke Mathematical Journal, (3) **132** (2006), 545-578.

[21] A. Brumer, *The average rank of elliptic curves I*, Invent. Math. **109** (1992), 445-472.

[22] L. Caporaso, J. Harris, B. Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), 1-35.

[23] B. Cook, A. Magyar, *Diophantine equations in primes*, Invent. Math. **198** (2014), 701-737.

[24] J. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **2** (1999), 64-94.

[25] P. Erdős, *Arithmetical properties of polynomials*, J. London Math. Soc. **28** (1953), 416-425.

[26] P. Erdős, K. Mahler, *On the number of integers which can be represented by a binary form*, J. London Math. Soc, **13** (1938), 134-139.

[27] J-H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **75** (1984), 561-584.

[28] E. Fouvry, J. Klüners, *On the negative Pell equation*, Ann. of. Math (3) **172** (2010), 2035-2104.

[29] F. Q. Gouvêa, B. Mazur, *The square-free sieve and the rank of elliptic curves*, Journal of the American Mathematical Society (1) **4** (1991), 1-23.

[30] A. Granville, *ABC allows us to count squarefrees*, International Mathematics Research Notices, **9** (1998).

[31] G. Greaves, *Power-free values of binary forms*, Q. J. Math, (2) **43** (1992), 45-65.

[32] D. R. Heath-Brown, *The density of rational points on curves and surfaces*, The Annals of Mathematics (2) **155** (2002), 553-598.

[33] D. R. Heath-Brown, *Counting rational points on algebraic varieties*, Analytic number theory, 5195, Lecture Notes in Math., 1891, Springer, Berlin, 2006.

[34] C. Hooley, *On the power free values of polynomials*, Mathematika **14** (1967), 21-26.

[35] C. Hooley, *On binary cubic forms*, J. reine angew. Math. **226** (1967), 30-87.

[36] C. Hooley, *On the numbers that are representable as the sum of two cubes*, J. reine angew. Math. **314** (1980), 146-173.

[37] C. Hooley, *On binary quartic forms*, J. reine angew. Math. **366** (1986), 32-52.

[38] C. Hooley, *On binary cubic forms: II*, J. reine angew. Math. **521** (2000), 185-240.

[39] C. Hooley, *On the power-free values of polynomials in two variables*, Analytic number theory, 235-266, Camb. Univ. Press, 2009.

[40] C. Hooley, *On the power-free values of polynomials in two variables: II*, Journal of Number Theory, **129** (2009), 1443-1455.

[41] E. Katz, J. Rabinoff, D. Zuerick-Brown, *Uniform bounds for the number of rational points on curves with small Mordell-Weil rank*, Duke. Math. J, **165** (2016), 3189-3240.

[42] B. Lawrence, A. Venkatesh, *Diophantine problems and p-adic period mappings*, arXiv:1807.02721 [math.NT].

[43] K. Mahler, *Zur Approximation algebraischer Zahlen. III. (Über die mittlere Anzahl der Darstellungen grosser Zahlen durch binäre Formen)*, Acta Math. **62** (1933), 91-166.

[44] R. Murty, H. Pasten, *Counting square free values of polynomials with error term*, International Journal of Number Theory, (7) **10** (2014), 1743-1760.

[45] B. Poonen, *Squarefree values of multivariate polynomials*, Duke Math. J., (2) **118** (2003), 353-373.

[46] P. Salberger, *Counting rational points on projective varieties*, Preprint 2009.

[47] P. Salberger, *Uniform bounds for rational points on cubic hypersurfaces*, Arithmetic and Geometry, Cambridge University press, 2015.

[48] A. Smith, $2^\infty$*-Selmer groups,* $2^\infty$*-class groups, and Goldfeld's conjecture*, arXiv:1702.02325 [math.NT].

[49] C. L. Stewart, *On the number of solutions of polynomial congruences and Thue equations*, J. Amer. Math. Soc, (4) **4** (1991), 793-835.

[50] C. L. Stewart, J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc, (4) **8** (1995), 943-972.

[51] M. Stoll, *Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank*, J. Eur. Math. Soc. (3) **21** (2019), 923-956.

[52] M. Walsh, *Bounded rational points on curves*, Int. Math. Res. Notices, Issue 14 Volume 2015, 5644-5658.

[53] M. E. M. Wood, *Moduli spaces for rings and ideals*, ProQuest LLC, Ann Arbor, MI, 2009, Ph.D. thesis, Princeton University.

[54] G. Yu, *Average size of 2-Selmer groups of elliptic curves, I*, Trans. Amer. Math. Soc **358** (2006), 1563-1584.